МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Алтайский государственный университет»
Юридический факультет

Кафедра уголовного права и криминологии

Региональный научно-методический центр правовой и технической защиты информации

ПРЕСТУПНОСТЬ ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ В СФЕРЕ ВЫСОКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: ПРИЧИНЫ, УСЛОВИЯ, ПРОФИЛАКТИКА

Учебное пособие

Барнаул
Издательство
Алтайского государственного
университета
2018

УДК 343.9.01
ББК 67.51
П 73

Редакторы:

Мазуров В.А., доцент кафедры уголовного права и криминологии Алтайского государственного университета, кандидат юридических наук, доцент, заместитель руководителя Регионального научно-методического центра правовой и технической защиты информации;

Куликов Е.А.,– доцент кафедры уголовного права и криминологии Алтайского государственного университета, кандидат юридических наук.

Рецензенты:

Детков А.П., доктор юридических наук, профессор, заведующий кафедрой уголовного права и криминологии Алтайского государственного университета;

Васильев А.А., доктор юридических наук, профессор, заведующий кафедрой теории и истории государства и права Алтайского государственного университета.

П 73 ***Преступность экстремистской и террористической направленности в сфере высоких информационных технологий: причины, условия, профилактика***: учебное пособие / под ред. В.А. Мазурова и Е.А. Куликова. – Барнаул: Изд-во Алт. гос. ун-та, 2018. — 154 с.

ISBN 978-5-7904-2292-8

Учебное пособие посвящено актуальной и недостаточно разработанной в отечественной криминологии тематике преступности в сфере информационных технологий, обладающей экстремистской и террористической направленностью. Рассматриваются общие вопросы, связанные с терроризмом, изучаются отдельные проявления экстремизма и терроризма в сфере высоких технологий, роль Интернета и социальных сетей в эволюции этих явлений в современном мире и т.д. Пособие подготовлено коллективом преподавателей, магистрантов и студентов юридического факультета Алтайского государственного университета.

Пособие будет полезно при изучении вопросов противодействия преступности экстремисткой и террористической направленности по криминологии и предназначено для студентов, магистрантов, аспирантов, адъюнктов, преподавателей, практических работников и всех, кто интересуется проблемами противодействия терроризму и экстремизму.

УДК 343.9.01
ББК 67.51

ISBN 978-5-7904-2292-8

СОДЕРЖАНИЕ

ПОНЯТИЕ ТЕРРОРИЗМА КАК СОЦИАЛЬНО-НЕГАТИВНОГО ЯВЛЕНИЯ

(Куликов Е.А., Суханова Е.П., Соколов А.С.)

Анализ отдельных вопросов, связанных с явлением «терроризм», предполагает предварительное рассмотрение сложившихся в современной науке подходов к понятию этого явления, и выработку на их основе рабочего варианта определения данного понятия. Это позволит определиться с предметным полем настоящего исследования и обозначить те рамки, в которых необходимо изучать проблемы противодействия экстремизму и терроризму в сфере высоких технологий. Настоящая глава, по этой причине, играет роль своеобразного введения в учебное пособие и призвана послужить обзором основных подходов к понятию и явлению «терроризм» в отечественной криминологии.

Традиционно рассмотрение явлений «террор», «терроризм», «преступления террористической направленности» начинают с обзора языковых сегментов искомых понятий, выяснения их этимологии и эволюции понимания на протяжении истории обществоведческих наук. На наш взгляд, природу терроризма и террора можно понять только исходя из их априорной криминальности, очевидной общественной опасности, что предопределяет рассмотрение этих явлений сначала с криминологических позиций, а уже затем выход на более высокие уровни абстракции.

Обратимся прежде всего к фундаментальному Курсу мировой и российской криминологии В.В. Лунеева, который выступает на сегодняшний день наиболее подробным исследованием криминологических проблем общего характера. Ученый отмечает в начале рассмотрения терроризма: «Бесспорно лишь то, что терроризм представляет собой особую разновидность политической преступности, кто бы её не совершал: власти, стремящиеся радикальным путем изменить существующий порядок в стране, или оппозиционеры (революционеры, националисты, религиозные фанатики, организованные преступники), жаждущие захвата и изменения власти или её существенных уступок»[1]. «Террористам важны не только и не столько объективные преступные последствия, сколько общественный, политический и международный резонанс, устрашение власти и населения, открытая демонстрация своей силы»[2]. Таким образом, В.В. Лунеев связывает терроризм и политическую преступность, рассматривает его как вид последней, как наиболее опасное проявление политической преступности, рассчитанное на внешний эффект, вызывающее существенные и значимые социальные последствия.

Ученый также проводит разграничение между терроризмом и национально-освободительной борьбой народов. «Основной трудностью для международного сообщества при выработке более или менее однозначного толкования терроризма было прямое или косвенное признание справедливости борьбы народов за свое

[1] Лунеев В.В. Курс мировой и российской криминологии в 2 т. Т. II. Особенная часть: учебник для вузов. – М.: Юрайт, 2013. С. 130-131.
[2] Там же. С. 132.

освобождение (независимость, суверенитет) при наличии противоречивых международно-правовых принципов (право наций на самоопределение, с одной стороны, и нерушимость существующих границ – с другой). Не способствовало выработке единого понимания и использование разными странами двойных стандартов при оценке действий тех или иных национальных, религиозных, политических и социальных групп населения. Руководство одной страны при оценке действий террористических образований, использующих крайнее насилие для достижения политических, сепаратистских, националистических и религиозных целей, признает их борьбой за свободу, а руководство другой страны считает эти действия терроризмом, - в зависимости от того, что удобнее в конкретной ситуации. Один из проблемных моментов – отграничение терроризма от освободительной и национально-освободительной борьбы. Терроризм, как правило, не носит массового характера, он замкнут на себя, узок и антидемократичен. В то же время если освободительная борьба – это убийство невинных мирных жителей, женщин и детей, то она ничем не отличается от терроризма»[3]. Весьма сложно говорить вообще о правильности и оправданности такого рода насилия, какими бы благими не были цели, они не могут оправдать те средства, которые используются для их достижения, вследствие чего терроризм всегда остается терроризмом, насилием, общественно опасным явлением, какие бы благие и правильные с точки зрения морали, религии или чьих-либо представлений о чести и достоинстве лозунги террористы не использовали.

В.В. Лунеев подразделяет терроризм на государственный, международный и внутренний. «Государственный терроризм (или государственный террор) предполагает террористическую деятельность самого государства против внутренних политических противников и в отношении иностранных государств для решения внутриполитических и внешнеполитических задач»[4]. Сложно применить по отношению к политике государства термин «терроризм», речь идет, скорее, о терроре, такого рода позиция в юридической литературе представлена и в дальнейшем мы её рассмотрим. Международный терроризм В.В. Лунеев определяет через специфику субъекта (террористические государства – государства, поддерживающие терроризм, и международные террористические организации), «внутренний терроризм также может осуществляться двумя субъектами: государством против своего народа и внутренними террористическими организациями и отдельными лицами против политических и экономических конкурентов»[5]. Соглашаясь в целом с этими формулировками, нельзя не заметить, что они носят предельно абстрактный характер и не показывают содержательную сторону терроризма.

Обстоятельное исследование проблематики террора, терроризма и преступлений террористического характера проводит С.У. Дикаев, в свете которого высказанные В.В. Лунеевым идеи наполняются определенным содержанием. Хотя его позиция

[3] Там же. С. 133-134.
[4] Там же. С. 136.
[5] См.: Там же. С. 137-138.

достаточно тенденциозна и несколько однобоко представляет поднимаемую проблему, она заслуживает к себе внимания. Вообще трудно себе представить исследование преступности террористической направленности, безотносительно точки зрения на неё, которое бы являлось стопроцентно объективным и беспристрастным. Религиозный, политический и иной духовный, нематериальный контекст идеологии терроризма и террора, как правило, определяет позицию того или иного ученого, занимающегося этими явлениями. Тем не менее, это не лишает ни одну научную работу методологической, содержательной и гносеологической ценности, в связи с чем каждая аргументированная позиция заслуживает к себе внимания. Особенно если речь идет о фундаментальном научном труде С.У. Дикаева «Террор, терроризм и преступления террористического характера».

Прежде всего, ученый предлагает разграничивать понятия «террор» и «терроризм». «Террор можно определить как социально-политическое явление, выражающееся в использовании субъектами, обладающими государственно-властными полномочиями, институтов государственной власти для реализации преступной политики, содержанием которой является систематическое применение насилия, экономическое угнетение населения, развязывание войн, преднамеренное уничтожение гражданских объектов, геноцид, экоцид, насильственная депортация, а равно иные действия, совершаемые с целью внушения населению постоянного чувства страха перед властью или отдельными органами государственной власти»[6]. Получается, что С.У. Дикаев связывает понятие «террор» с деятельностью государства, государственной власти и характеризует его как, своего рода, государственную политику, осуществляемую крайними, недопустимыми насильственными и устрашающими средствами.

По поводу определения понятия терроризма ученый высказывает довольно любопытные соображения, в частности, говоря о том, что «многочисленные попытки ученых дать строгое определение терроризма не увенчались успехом, и мы склоняемся к мысли, что терроризм, подобно множеству в математике, следует рассматривать как неопределяемое понятие, а главное, к чему нужно стремиться и что нужно сделать, - это определить его границы, облегчив тем самым разрешение уголовно-правовых отношений… терроризм – это более узкое понятие, чем террор, и его можно рассматривать как практическую реализацию постулата о том, что сходное должно вызывать сходное. И дело не только в стремлении противоборствующих сил причинять смерть, разрушения, производить ужасающие эффекты и т.д. Представляется совершенно логичным и даже неизбежным, что постоянное увеличение силы увеличивает и желание эту силу разрушить»[7]. Терроризм С.У. Дикаев предлагает понимать как ответную реакцию на государственный террор, как действия негосударственных образований, применяющих насилие в целях защиты собственных интересов. Такая позиция заслуживает внимания, поскольку речь идет

[6] Дикаев С.У. Террор, терроризм и преступления террористического характера (криминологическое и уголовно-правовое исследование). – СПб.: Юридический центр «Пресс», 2006. С. 43.
[7] Там же. С. 43.

не просто о схоластическом разведении понятий, обозначающих, по сути, одно и то же, а о содержательном разграничении террора и терроризма как разных, и даже противоположных социально негативных явлений. В дальнейших рассуждениях С.У. Дикаев исходит именно из такого разграничения понятий «террор» и «терроризм» и обозначаемых ими явлений.

Мы не будем останавливаться на видах террора и терроризма, поскольку этот вопрос находится за рамками предмета данного раздела исследования. Необходимо, однако, рассмотреть специфические черты терроризма, выделяемые С.У. Дикаевым. Обобщая представленные в юридической литературе содержательные и динамические характеристики терроризма, С.У. Дикаев называет следующие его особенности:

1. Чрезвычайно расширилась география терроризма, он распространился на все регионы мира. При этом, несмотря на определенные спады и подъёмы террористической деятельности в различных странах, практически терроризм уже в течение полувека не уходит из регионов большой террористической активности, превратившись в долговременный фактор общественной жизни, в неотъемлемый элемент политической борьбы.

2. Значительно расширился круг субъектов терроризма. Наряду с ростом числа террористических организаций в системе субъектов терроризма значительную роль стали играть качественно новые структуры: а) международные террористические организации, возникшие в результате межгосударственных конфликтов; б) структуры организованной преступности, многие из которых приобрели международный характер и преследуют корыстные цели; в) субъекты террористической деятельности, которые связаны с крупными социальными конфликтами и массовыми действиями вовлеченных в них групп и лиц (участники массовых беспорядков, межнациональных столкновений, протестных «экологических» акций и др.).

3. Значительно изменился характер и расширился круг целей и задач террористических структур («свержение режима», «изгнание» иностранной державы, «атака на империализм» и т.д.).

4. Качественно возрос насильственный и разрушительный потенциал терроризма. Имеется ввиду не столько увеличение числа жертв террористических акций или нарастание чувства страха и опасности среди широких слоев населения в различных регионах мира, сколько уровень вооруженности террористов, повышение которого обусловлено научно-техническим прогрессом, принципиальными достижениями в создании средств массового поражения.

5. Терроризм приобрел высокоорганизованный характер (у него сформировалась собственная инфраструктура, появилась разветвленная сеть штаб-квартир, опорных пунктов, лагерей по подготовке террористов, постоянная связь с экстремистскими политическими движениями и партиями, постоянные каналы финансирования и т.д.).

6. Субъекты терроризма способны воздействовать практически на все сферы общественных отношений в различных регионах мира.

7. Резко возросло число возможных и реальных жертв террористических акций за счет «случайных» лиц, т.е. терроризм приобрел качество инструмента более массового насилия и устрашения. Это связано, прежде всего, с появлением в арсенале террористов средств большой мощности, не требующих для своего применения непосредственного контакта террориста с объектами посягательства, с увеличением числа террористов-самоубийц, а также с наличием установки на повышение устрашающего воздействия актов терроризма на политических противников, на общественное мнение, что должно повысить вероятность решения поставленных террористами задач.

Главной же особенностью терроризма современного периода следует считать то, что он значительно шире, чем когда-либо, используется в политической борьбе, на международной арене в целом и между отдельными государствами в частности[8].

Также нужно обратить внимание на понятия межгосударственного и международного терроризма, определяемые С.У. Дикаевым, поскольку как мы видели выше, В.В. Лунеев подобные термины не раскрывает, а лишь намечает их в общих чертах. «Международный терроризм – это совершение актов терроризма одной социальной группой, объединенной по этническому или национальному признаку, против представителей другой социальной группы, объединенной по этническому или национальному признаку, обусловленное национальной, расовой, религиозной или культурной нетерпимостью»[9]. Получается, что ученый определяет международный терроризм исходя из смысла слова «народ», как терроризм, выступающий средством осуществления конфликтов между народами. Это довольно нетривиальная и вполне логичная трактовка. К признакам такого терроризма С.У. Дикаев относит: 1) акт терроризма совершается на почве неприязненных межгрупповых отношений, связанных с социальным или политическим конфликтом; 2) субъекты терроризма и их жертвы являются представителями разных народов, проживающих на территории одного государства, гражданами которого они являются; 3) субъекты терроризма и их жертвы являются представителями разных народов, проживающих на территории более чем одного государства, обладают гражданством разных государств, при отсутствии признаков, указывающих на провоцирующую роль государства[10].

«Межгосударственный терроризм – это невоенные насильственные действия одного субъекта межгосударственного (международного) права, совершенные в целях ослабления политических, экономических, идеологических и иных позиций другого субъекта межгосударственного (международного) права»[11]. К признакам этого терроризма относятся: 1) акт терроризма осуществляется с санкции одного государства против объектов другого государства; 2) между государствами нет

[8] Дикаев С.У. Террор, терроризм и преступления террористического характера (криминологическое и уголовно-правовое исследование). – СПб.: Юридический центр «Пресс», 2006. С. 171-172.
[9] Там же. С. 53-54.
[10] См.: Там же. С. 54.
[11] Дикаев С.У. Террор, терроризм и преступления террористического характера (криминологическое и уголовно-правовое исследование). – СПб.: Юридический центр «Пресс», 2006. С. 54.

отношений, вызванных объявлением войны; 3) целью акции является ослабление политических, экономических, идеологических и иных позиций другого государства или провокация внутреннего конфликта. Главные особенности межгосударственного терроризма: 1) как правило, он носит совершенно секретный характер; 2) государства отрицают свою причастность к актам терроризма и обвиняют в них противоположную сторону; 3) террористические действия осуществляются спецслужбами государства непосредственно или уже путем вербовки и вооружения террористов; 4) опекаемые государствами террористы лучше обеспечивают государственные интересы одним эффективным актом терроризма, чем армейские подразделения военными операциями[12]. Здесь, как видим, речь идет об определенного рода взаимодействиях между субъектами международного права, в качестве которых С.У. Дикаев рассматривает только государства.

Думается, при разграничении международного и межгосударственного терроризма, следуя намеченному С.У. Дикаевым подходу, можно ввести такой критерий, как наличие, либо отсутствие государственного сегмента в террористических действиях. Возможны и промежуточные формы, когда сталкиваются какой-либо народ и государство, представляющее интересы другого народа. В качестве недостатка такого подхода можно отметить то, что на сегодняшний день международный терроризм и межгосударственный терроризм крайне сложно разграничить, так или иначе они могут находиться на одном уровне, или на разных. Следуя логике В.В. Лунеева, можно выделять международный терроризм на внутригосударственном и межгосударственном уровне. Внутри государства в состоянии террористического противостояния могут находиться титульная нация и угнетенные народы, на межгосударственном – народ одного государства с народом другого государства. Терроризм же с государственным сегментом нуждается в дополнительном уточнении о пределах государственного руководства таким терроризмом.

К сказанному С.У. Дикаевым по поводу отличительных черт современного терроризма следует добавить ещё и то, что при исследовании современного терроризма необходимо учитывать практически повсеместную «виртуализацию» социальной жизни (по крайней мере, в определенной части стран, относящихся к т.н. западной цивилизации) в городах, значительную урбанизацию населения, и связанное с этим кардинальное изменение характера и содержания коммуникаций между людьми, что меняет и содержание терроризма. На сегодняшний день эта ситуация породила такие явления, как виртуальный терроризм, кибертерроризм, Интернет-терроризм, коммуникационные системы (социальные сети, мессенжеры и т.п.) становятся важными каналами связи в т.ч. и для деятельности террористов и «сочувствующих», что, в свою очередь, требует и от тех, кто готовит научное обоснование политики противодействия терроризму, учета такого характера преступности террористической направленности в наши дни. Это с одной стороны.

[12] См.: Там же. С. 54.

С другой стороны, на наш взгляд, меняется, по большому счету, только форма, средства обеспечения и взаимодействия, а также масштабы жертв и разрушений, т.е. имеют место исключительно количественные трансформации терроризма. Что касается качественной стороны – сущности этого социально негативного явления, комплекса его детерминант и личностных особенностей террористов, - то эта сторона в основе своей не особенно изменилась со времен возникновения терроризма как явления. Это по прежнему метод борьбы, метод воздействия, метод получения нужных решений, основанный исключительно на насилии и причинении вреда социально значимым ценностям, не связанным напрямую с целями террористов, но достаточно значимым, чтобы их повреждение, либо угроза такового, могли склонить нужного субъекта на принятие нужного террористам решения. Хотя, разумеется, конкретные свойства и отдельные проявления у терроризма XIX века и терроризма XXI века различаются.

Ю.С. Горбунов отмечает, что уже во времена Римской империи в понятие «террор» вкладывался конкретный смысл: устрашение политического оппонента (противника) насильственными методами, вплоть до физического устранения отдельных его представителей, в целях управления поведением этого оппонента (противника) – то есть то, что сегодня присуще дефиниции «терроризм». «Указанные особенности – систематическое устрашение политического оппонента различными методами с целью управления им и (или) связанных с ним лиц – являются сущностными отличиями терроризма, позволяющими отграничить терроризм от других видов насилия. Эти особенности свидетельствуют об изначально сложной структуре объекта террористических посягательств и политической его мотивации»[13]. Невозможно не согласиться с последним утверждением автора. В то же время Ю.С. Горбунов считает, что проводимые в литературе различия между понятиями «террор» и «терроризм» являются, ввиду этимологии этих терминов, надуманными[14]. Выше мы уже отмечали, что сама по себе этимология далеко не всегда может определять со стопроцентной точностью современное значение того или иного слова, в различении же террора и терроризма состоит, прежде всего, представление о существовании различных явлений – террора со стороны государства и терроризма со стороны его противников как своеобразного ответа на политику террора. В силу этого позиция Ю.С. Горбунова по данному вопросу нам видится не вполне точной.

Обстоятельная критика смешения понятий террора и терроризма, а также критерии их разграничения приводятся в монографии Е.А. Капитоновой и Г.Б. Романовского. Во-первых, терроризм представляет собой разовый акт либо серию подобных актов, тогда как террор носит тотальный, массовый и непрерывный характер. В результате крупнейших терактов может погибнуть куда меньше людей, чем в ходе осуществления террора. Планомерность действий при терроре обеспечивает больший круг жертв и продолжительность воздействия на людей

[13] Горбунов Ю.С. Терроризм и правовое регулирование противодействия ему: монография. – М.: Молодая гвардия, 2008. С. 16-17.
[14] См.: Там же. С. 17.

(может длиться даже не днями и неделями, а годами). Во-вторых, субъекты терроризма, в отличие от субъектов террора, не наделены никакими властными полномочиями. Они в любом случае не располагают официально установленной властью над жителями той местности, где ими совершаются преступления. Субъектами же террора всегда выступают представители государственной власти. При этом совсем не важно, каким именно образом (выборным путем, военной интервенцией, узурпацией или в порядке престолонаследия) они эту власть получили. В-третьих, субъектами террора выступают общественно-политические структуры (стоит добавить, что также и отдельные должностные лица), а субъектами терроризма – физические вменяемые лица, достигшие возраста уголовной ответственности, вне всяких специальных признаков субъекта преступления. В-четвертых, существенным образом различаются цели, которых желают достичь субъекты рассматриваемых действий. При терроре устрашение населения осуществляется с целью понуждения к определенному поведению самого населения. Страх выступает для наделенных властными полномочиями лиц способом удержать людей в повиновении, добиться от них смирения и принятия проводимой в государстве политики. Субъекты терроризма осуществляют устрашение населения совсем с другой целью. Их мало интересует повиновение жертв и тем более принятие ими террористических идей. Люди, страдающие в результате теракта, служат лишь средством, а не объектом воздействия. Настоящей же целью терроризма является понуждение к определенному поведению представителей власти или международной организации. Таким образом, воздействие на конечного адресата производится опосредованно – не путем создания страха за свою собственную жизнь, а посредством формирования чувства ответственности за судьбы других людей. В-пятых, террор – это социально-политический фактор действительности, а терроризм – уголовно-наказуемое деяние. В этом заключена и разница в оценке рассматриваемых действий в процессе их совершения. Теракты повсеместно считаются общественно опасными деяниями, за совершение которых предусмотрено наказание. Жертв терроризма защищает государство, где они проживают, и даже мировое сообщество в целом. Их права признаются, за их жизни, условно говоря, есть кому бороться. В случае террора негативно оценивать происходящее с ними могут только сами жертвы. При этом они вряд ли найдут поддержку и защиту своих прав у властных структур, поскольку именно эти структуры, как правило, и осуществляют террор. Оценка совершенных в процессе террора деяний как преступных возможна только после изменения политики на данной территории. Происходит это обычно со сменой власти либо при резком изменении ориентиров социально-политического развития государства[15].

Как видим, существует, как минимум, пять оснований для разграничения между собой террора и терроризма. Приведенная позиция Е.А. Капитоновой и Г.Б. Романовского позволяет вывести ряд промежуточных следствий. Прежде всего, понятно, что область террора, терроризма и преступлений террористической

[15] См. подробнее: Капитонова Е.А., Романовский Г.Б. Современный терроризм: монография. – М.: Юрлитинформ, 2015. С. 29-31.

направленности, как, в общем-то, и любая политически и идеологически ангажированная область социальной жизни, всегда была и остается сферой проявления двойных стандартов, разного рода условностей, принципа «свои – чужие», «революционеры – реакционеры» и т.п., где многое определяется именно точкой зрения. Чего стоят одни труды Н.А. Троицкого по истории народовольческого терроризма. В связи с этим очень важно различать террор и терроризм, определять каждое понятие самостоятельно исходя из общественной опасности и того, и другого явления. С другой стороны, это же означает, что и государственный террор, и антигосударственный терроризм одинаково социально опасны. Цель не может оправдать такие средства её достижения, и цена, которую заплатит общество при достижении этой цели или при частичном получении результатов, просто несоизмерима с эфемерным «светлым будущим», что мы наблюдаем на примере отечественной истории XIX-XXI вв.

Для того чтобы рассмотрение нами вопроса о понятии терроризма приобрело хотя бы относительную полноту, нужно обратить внимание на существующую на сегодняшний день в России легальную трактовку этого понятия. «Терроризм – идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий» - такое определение дается в статье 3 Федерального закона от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму». Законодатель, таким образом, подчеркнул двойственную природу терроризма как социально-негативного явления: это определенная идеология насилия и это определенная практика, и объединяет их цель воздействия на властные структуры, а также связь с устрашением населения и иными противоправными насильственными действиями. При всей сложности и многоплановости явления «терроризм» в этой части он предельно понятен и занимает определенное место среди общественно опасных явлений социальной жизни.

Как уже выше мы отмечали, в современных условиях на преступность террористической направленности и другие проявления накладывают свой отпечаток развитие массовых коммуникаций, глобальных электронных средств связи, сказывается распространенность социальных сетей и их роль в жизни «среднего» человека. Участники движений террористического характера активно используют эти достижения современной цивилизации, в связи с чем для формировании стратегии профилактики терроризма в новых условиях необходимо учитывать этот «виртуальный» фактор. По этой причине настоящее пособие специально посвящено проявлениям терроризма и экстремизма в сфере высоких технологий.

ЭКСТРЕМИЗМ В СОЦИАЛЬНЫХ СЕТЯХ: ПРИЧИНЫ, УСЛОВИЯ, ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ПРОФИЛАКТИКИ (*Л.Н. Бырдина*)

Введение. Современный экстремизм с точки зрения управления и организации совершенствуется не менее стремительно, чем новейшие технологии. Динамичное развитие сети «Интернет» с его простотой доступа, относительно низкой стоимостью, анонимностью, незначительным масштабом государственного регулирования и цензуры, потенциально огромными масштабами аудитории, быстрой передачей информации, мультимедийностью среды дает современным экстремистам огромные возможности для осуществления экстремисткой деятельности, наиболее ярко проявляющейся в социальных сетях. Именно в виртуальном мире экстремисты получают недопустимую в реальном обществе свободу и становятся не столько потребителями, сколько создателями экстремистских материалов. Экстремисты активно используют социальные интернет-сети для ведения идеологической пропаганды, координации и планирования своей противоправной деятельности, а так же достижения преступных целей, направленных на возбуждение ненависти или вражды. Вместе с тем, массовая распространенность и повсеместное использование информационных технологий чрезвычайно затрудняет поиск и обнаружение экстремистских групп, их активных и тайных участников. Учитывая данные официальной статистики, можно уверенно говорить о росте преступности в данном сегменте и постепенном укреплении данного негативного явления в нашей стране, что обуславливает необходимость наиболее полного его изучения.

Тема экстремизма в социальных сетях широко изучена не только специалистами в области юриспруденции, но и в социологии, психологии, педагогики, политологии и т.д. Наиболее детально данная тематика проработана в исследованиях следующих авторов: С.А. Перчаткиной, М.Е. Черемисиновой, А.М. Цирина, М.А. Цириной, Ф.В. Цомартовой[16]; Е.П. Сергуна[17], И.С. Макеевой[18]; А.В. Смагиной, Д.И. Сапун[19], Е.В. Реутова[20], В.А. Лелекова, А.А. Черных[21], Н.А. Морозовой[22], В.В. Степанова, А.В. Струкова[23], К.В. Бедарева[24], С.А. Кузнецова, С.М. Оленникова[25], Н.Н. Телешиной[26],

[16]Перчаткина С.А., Черемисинова М.Е., Цирин А.М., Цирина М.А., Цомартова Ф.В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2012. № 5.
[17]Сергун Е.П. Экстремизм в российском уголовном праве: Автореферат диссертации на соискание ученой степени кандидата юридических наук. Тамбов, 2009.
[18]Макеева И.С. Экстремизм как уголовно-правовая категория // Законодательство и экономика. 2014. № 6.
[19]Смагина А.В., Сопун Д.И. Причины распространения экстремизма в России // Российский следователь. 2012. № 8.
[20]Реутов Е. В. Причины распространения экстремизма и ксенофобии в молодежной среде. Белгород, 2008.
[21]Лелеков В.А., Черных А.А. О причинах преступлений экстремистской направленности в молодежной среде // Российский следователь. 2015. № 8.
[22]Морозова Н.А. Проблемы привлечения к уголовной ответственности за экстремизм в информационной сети Интернет // Российский следователь. 2014. № 5.
[23]Степанов В.В., Струков А.В. Проблемы разрешения конкуренции составов преступлений экстремистской направленности // Вестник Пермского университета. Юридические науки. 2015. № 1.

А.Б. Смушкина[27], В.А. Авдеева, О.А. Авдеевой[28], М.В. Залоило, Н.В. Власовой[29], М.А. Беловой, Н.Э. Рустамова[30], С.В. Борисова, А.А. Чургунова[31], В. Михайлова[32], С.А. Кузнецова, С.М. Оленникова[33], Л.В. Григорьевой[34].

Правовую базу исследования составили: Конституция Российской Федерации[35], Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом[36], Резолюция Парламентской Ассамблеи Совета Европы 1344 (Принятая в 2003 г) «Об угрозе для демократии со стороны экстремистских партий и движений в Европе»[37]; Федеральные законы – «О противодействии экстремистской деятельности»[38], «Об информации, информационных технологиях и о защите информации»[39], «Об оперативно-розыскной деятельности»[40]; Кодексы – Уголовный кодекс Российской Федерации[41], Кодекс об административных правонарушениях Российской Федерации[42]; Указы Президента Российской Федерации – «О Стратегии

---

[24]Бедарев К.В. Противодействие преступлениям, совершаемым по мотивам расовой, национальной или религиозной ненависти или вражды в сети Интернет. Краснодар. 2015.

[25]Кузнецов С.А., Оленников С.М. Экспертные исследования по делам о признании информационных материалов экстремистскими: теоретические основания и методическое руководство (научно-практическое издание). М., 2014.

[26]Телешина Н.Н. К вопросу о совершенствовании государственного контроля виртуального пространства // Информационное право. 2012.№ 1.

[27] Смушкин А.Б. Комментарий к Федеральному закону от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // СПС.КонсультантПлюс. 2015.

[28] Авдеев В.А., Авдеева О.А. Механизм противодействия преступлениям террористического характера и экстремистской направленности в Российской Федерации // Юридический мир. 2014. № 12.

[29]Залоило М.В., Власова Н.В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5.

[30]Белова М.А., Рустамов Н.Э. Правовые средства противодействия экстремизму по российскому праву // Административное и муниципальное право. 2015. № 1.

[31]Борисов С.В., Чугунов А.А. Новеллы уголовного законодательства в сфере противодействия экстремизму: критический анализ // Современное право. 2015. № 4.

[32]Михайлов В. Процедура признания материалов экстремистскими требует коррекции // Административное право. 2015. № 1.

[33]Кузнецов С.А., Оленников С.М. Экспертные исследования по делам о признании информационных материалов экстремистскими: теоретические основания и методическое руководство (научно-практическое издание). М., 2014.

[34]Григорьева Л.В. О научном подходе к уголовно-правовой оценке действий экстремистской направленности // Современное право. 2015. № 7.

[35] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрании законодательства РФ.- 04 августа.- 2014.- № 31.Ст. 4398.

[36]Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом (заключена в г. Шанхае 15.06.2001) // Собрание законодательства РФ. 2003. 13 октября. № 41. Ст. 3947.

[37] Резолюция Парламентской Ассамблеи Совета Европы 1344 (Принята в 2003 г) «Об угрозе для демократии со стороны экстремистских партий и движений в Европе».

[38] О противодействии экстремистской деятельности: Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 23.11.2015) // Российская газета.- 30 июля.- 2002.- 138-139.

[39] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 13.07.2015) // Российская газета.- 29 июля.- 2006.- № 165.

[40]Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.06.2015) // Российская газета.- 18 августа.- 1995.- № 160.

[41] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.11.2015) // Собрание законодательства РФ.- 17 июня.- 1996.- № 25. Ст. 2954.

[42]Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 14.12.2015) // Российская газета.- 31 декабря.- 2001.- № 256.

национальной безопасности Российской Федерации»[43], «Вопросы Министерства юстиции Российской Федерации»[44]; Определение Конституционного Суда Российской Федерации «Об отказе в принятии к рассмотрению жалобы гражданина Кочемарова Владислава Сергеевича на нарушение его конституционных прав положениями пунктов 1 и 3 статьи 1 и части третьей статьи 13 Федерального закона «О противодействии экстремистской деятельности»[45]; Постановление Пленума Верховного Суда Российской Федерации «О судебной практике по уголовным делам о преступлениях экстремистской направленности»[46]; Приказ Министерства внутренних дел Российской Федерации «О деятельности органов внутренних дел по предупреждению преступлений»[47]. Кроме того, в исследовательской работе были использованы данные официальной статистики о состоянии преступности, представленные в краткой характеристике состояния преступности в Российской Федерации за январь - декабрь 2013, 2014, 2015 гг[48], и информационно-аналитических материалах к отчету начальника Главного управления МВД России по Алтайскому краю генерал-лейтенанта полиции Торубарова Олега Ивановича перед депутатами Алтайского краевого Законодательного Собрания за 2013 – 2015 гг[49].

При написании настоящей работы были применены общие и частные методы исследования, в том числе методы теоретического анализа литературы и нормативно-правовой базы, структурный и системный методы познания, сравнительный метод, а так же, классификация и группировка.

Научная значимость бакалаврской работы заключается в анализе состояния преступности экстремистского характера в социальных сетях, выявлении причин ее активного распространения. С практической точки зрения выводы о приоритетных направлениях профилактики могут быть использованы правоприменителем в борьбе с преступлениями в изучаемом сегменте.

Исследовательская работа состоит из введения, трех глав, заключения, списка источников и литературы, приложения. Во введении обоснована актуальность темы, обозначены цель, задачи, объект, предмет, методы; отмечены научная, практическая

---

[43]О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31.12.2015 // Собрание законодательства РФ.- 04 января.- 2016.- № 1 (часть II). Ст. 212.

[44]Вопросы Министерства юстиции Российской Федерации: Указ Президента РФ от 13.10.2004 № 1313 (ред. от 31.12.2015) // Российская газета.- 19 октября.- 2004.- № 230.

[45] Об отказе в принятии к рассмотрению жалобы гражданина Кочемарова Владислава Сергеевича на нарушение его конституционных прав положениями пунктов 1 и 3 статьи 1 и части третьей статьи 13 Федерального закона «О противодействии экстремистской деятельности»: Определение Конституционного Суда РФ от 02.07.2013 N 1053-О // Вестник Конституционного Суда РФ.- 2014.- № 2.

[46] О судебной практике по уголовным делам о преступлениях экстремистской направленности: Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 // Бюллетень Верховного Суда РФ.- август.- 2011.- № 8.

[47]О деятельности органов внутренних дел по предупреждению преступлений: Приказ МВД России от 17.01.2006 № 19 (ред. от 30.12.2011) // СПС. КонсультантПлюс. 2015.

[48]Краткая характеристика состояния преступности в Российской Федерации, в том числе в Крымском федеральном округе за январь - декабрь 2015 года. [Электронный ресурс]: Статистические сведения / Официальный сайт МВД РФ.: МВД РФ, 2016. - Режим доступа: https://mvd.ru/folder/101762/item/7087734/

[49]Информационно-аналитические материалы к отчету начальника Главного управления МВД России по Алтайскому краю генерал-лейтенанта полиции Торубарова Олега Ивановича перед депутатами Алтайского краевого Законодательного Собрания [Электронный ресурс]: Отчеты перед населением / Официальный сайт МВД РФ.: МВД РФ,2015.-Режим_доступа: https://22.mvd.ru/Dejatelnost/otchnas/Otcheti_za_2014_god/Otchet_nachalnika_Glavnogo_upravlenija_M

значимость работы и определена структура. В первой главе дана общая характеристика экстремизма в социальных сетях, путем раскрытия понятийного аппарата, специфики данного вида преступлений, анализа данных официальной статистики, свидетельствующих о постоянном росте преступлений экстремистской направленности, совершаемых в сети «Интернет». Во второй главе рассмотрены причины и условия развития экстремизма в социальных сетях, предложена их классификация. В третьей главе изучены направления профилактики, определены субъекты, осуществляющие деятельность в данном направлении, представлены предложения исследователей данной области по решению вопроса борьбы с экстремизмом в социальных сетях. В заключении подведены общие итоги бакалаврского исследования, изложены основные выводы.

Экстремизм в социальных сетях: общая характеристика. В условиях глобального развития социально-экономической и общественной жизни на основе информационно-коммуникационных технологий массовое распространение киберпространства, на сегодняшний день, создающего новую реальность как для индивидов и организаций, так и для государств очевидно. В рамках интернет-пространства протекают активные информационно-коммуникационные процессы между лицами, образующими саморегулируемые интернет-сообщества, наиболее распространенной формой проявления которых в настоящее время являются социальные сети. Социальная интернет-сеть представляет собой страницу в сети «Интернет», поэтому, давая характеристику данной категории, следует прежде всего обратиться к Федеральному закону от 27 июля 2006 г № 149-ФЗ «Об информации, информационных технологиях и о защите информации», так как он содержит определение термина «сайт». Основные акценты в этом определении сделаны на трех составляющих сайта: содержание (информация, контент), технические (программные) средства, а также наличие доменного имени и (или) сетевого адреса[50]. Известный исследователь этой области Д. Бойд предложил следующее определение социальной сети: « - это сетевые услуги, которые позволяют частным лицам: строить общественные или полуобщественные профили в пределах ограничений, наложенных системой; определять список других пользователей, с которыми они могут сообщаться и делиться информацией; просматривать и связывать их список контактов с другими, созданными пользователями внутри системы»[51]. Таким образом, социальные сети позволяют, во-первых, выстраивать новые общественные связи путем свободного выбора пользователем круга общения и членства в интересующих его сообществах. Участник самостоятельно формирует группу, что позволяет, с психологической точки зрения, воспринимать свою страницу как личное пространство и, следовательно, проявлять большее доверие информации, циркулирующей в социальной сети, чем информации полученной из иных источников. Во-вторых, интерфейс социальной сети предоставляет участнику

[50] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 13.07.2015) ст. 2 // Российская газета.- 29 июля.- 2006.- № 165.
[51]Перчаткина С.А., Черемисинова М.Е., Цирин А.М., Цирина М.А., Цомартова Ф.В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2012. № 5. С. 14 - 24.

возможность наполнять ресурс своим контентом, вести блоги, которые свободно могут комментироваться другими участниками социальной сети. Это позволяет рассматривать социальную сеть не просто как средство общения, а как телекоммуникационную платформу массового распространения информации. В-третьих, современное развитие социальных сетей позволяет с полной уверенностью характеризовать их как трансграничное виртуальное общение, скорость которого не уступает «живому» общению вне сети. Ряд исследователей рассматривают возрастающее значение виртуальных социальных сетей как одну из глобалистских тенденций, обусловленную особенностями развития общественных отношений на современном этапе[52].Указанные свойства социальных сетей объясняют все возрастающее использование экстремистами сети «Интернет» в своей противоправной деятельности приоритетными направлениями которого являются: поиск и вербовка как пассивных, так и активных сторонников; массовое распространение заведомо экстремистских материалов; публичные призывы к осуществлению экстремистской деятельности; создание сетей; координация и планирование своей противоправной деятельности; осуществление контроля за фактическим проведением каких-либо мероприятий; а также поиск спонсоров, поддерживающих их радикальные идеи. Необходимо отметить, что на сегодняшний день экстремисты в социальных сетях не ограничиваются только размещением текстовых, графических, аудио-видео файлов, пропагандирующих экстремистскую деятельность. Данные субъекты ведут активный поиск, системный анализ и мониторинг пользователей, просматривающих их сайты. С наиболее подходящими лицами, с точки зрения вербовщиков, устанавливается контакт с целью дальнейшего их привлечения к осуществлению экстремистской деятельности.

Понятие экстремисткой деятельности закреплено в ряде нормативных правовых акта, в том числе и международных, однако единого подхода к толкованию данной категории нет. Так Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июня 2001 г, стороной-участницей которой является Российская Федерация, определяет экстремизм как: «какое-либо деяние, направленное на насильственный захват власти или насильственное удержание власти, а также на насильственное изменение конституционного строя государства, а равно насильственное посягательство на общественную безопасность, в том числе организацию в вышеуказанных целях незаконных вооруженных формирований или участие в них, преследуемые в уголовном порядке в соответствии с национальным законодательством Сторон»[53]. При этом названная Конвенция исходит из того, что перечисленные явления представляют угрозу международному миру и безопасности, развитию дружественных связей между государствами, а также осуществлению основных прав и свобод человека, серьезно угрожают территориальной целостности, безопасности и политической, экономической и социальной стабильности и не могут

[52]Там же.
[53] Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом (заключена в г. Шанхае 15.06.2001) // Собрание законодательства РФ. 2003. 13 октября. № 41. Ст. 3947.

быть оправданы ни при каких обстоятельствах. Поэтому рассматриваемый международный акт не только не препятствует государствам-участникам предусматривать в своем законодательстве положения о более широкой интерпретации экстремизма, но и обязывает их принимать все необходимые меры для обеспечения того, чтобы терроризм, сепаратизм и экстремизм ни при каких обстоятельствах не подлежали оправданию по соображениям исключительно политического, философского, идеологического, расового, этнического, религиозного или иного аналогичного характера и влекли наказание сообразно степени их тяжести.

Парламентской Ассамблеей Совета Европы по изучаемому вопросу в 2003 году была принята Резолюция 1344 «Об угрозе для демократии со стороны экстремистских партий и движений в Европе». Данный международный акт, обращая внимание на необходимость законодательного ограничения свободы выражения мнений, собраний и объединений, для целей борьбы с экстремизмом, подчеркивает, что независимо от своей природы экстремизм представляет собой форму политической деятельности, явно или исподволь отрицающую принципы парламентской демократии и основанную на идеологии и практике нетерпимости, отчуждения, ксенофобии, антисемитизма и ультранационализма[54].

Российским законодателем в Федеральном законе от 25 июля 2002 г № 114-ФЗ «О противодействии экстремистской деятельности» была предпринята попытка дать более точное и развернутое определение экстремистской деятельности, понятие которой, исходя из положений указанного нормативного акта, идентично понятию «экстремизм». Согласно ч. 1 ст. 1 Федерального закона экстремистская деятельность (экстремизм) – это: насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; публичное оправдание терроризма и иная террористическая деятельность; возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения; воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения; совершение преступлений по мотивам, указанным в пункте «е» части первой статьи 63 Уголовного кодекса Российской Федерации;пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени

[54] Резолюция Парламентской Ассамблеи Совета Европы 1344 (Принята в 2003 г) «Об угрозе для демократии со стороны экстремистских партий и движений в Европе» п. 3.

смешения, либо публичное демонстрирование атрибутики или символики экстремистских организаций; публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения; публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением; организация и подготовка указанных деяний, а также подстрекательство к их осуществлению; финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг[55]. Приведенное выше перечисление трудно назвать четким определением изучаемой дефиниции. Очевидно, что законодатель установил категорию «экстремизм» через перечень действий, относящихся к экстремистской деятельности. Однако данный подход подвергается активной критике со стороны ряда экспертов-юристов. Так Е.П. Сергун считает, что приведенное в Федеральном законе определение настолько широко, что даже образно представить круг перечисленных деяний весьма затруднительно[56]. Ученый определяет экстремизм как приверженность к определенной системе взглядов и идей, основанной на нетерпимости к основополагающим принципам конституционного строя Российской Федерации и охраняемым государством демократическим правам и свободам человека и гражданина, характеризующуюся внутренней готовностью к активной деятельности, направленной на претворение в действительность таких воззрений уголовно наказуемыми способами. Е.Б. Кургузкина так же обращает внимание на то, что понятие «экстремизм» данное в Законе, содержит явно завышенное количество перечислений, во многом частного характера, ряд из которых нельзя отнести к существенным признакам дефиниции[57]. Противоположной точки зрения придерживается И.С. Макеева, по мнению которой позиция законодателя вполне оправдана и объяснима. «Для всех форм исследуемого феномена, – утверждает она, – характерно наличие внутреннего побуждения, вызывающего у лица решимость совершить то или иное действие, а именно мотив политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо мотив ненависти или вражды в отношении какой-либо социальной группы. Наличие определенного мотива (несмотря на то что отдельные формулировки не содержат прямого указания на него) является главным критерием, объединяющим все

[55] О противодействии экстремистской деятельности: Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 23.11.2015) ч. 1 ст. 1 // Российская газета.- 30 июля.- 2002.- 138-139.
[56]Сергун Е.П. Экстремизм в российском уголовном праве: Автореферат диссертации на соискание ученой степени кандидата юридических наук. Тамбов, 2009. С. 8.
[57] Макеева И.С. Экстремизм как уголовно-правовая категория // Законодательство и экономика. 2014. № 6. С. 61 - 68.

перечисленные в статье 1 Закона № 114-ФЗ формы проявления экстремизма.»[58]. Принимая во внимание существующую теоретическую дискуссию по данному вопросу, при изучении экстремизма в первую очередь необходимо руководствоваться легальным определением данной дефиниции, закрепленным нормативными правовыми актами Российской Федерации. Помимо рассмотренного выше Федерального закона от 25 июля 2002 г № 114-ФЗ «О противодействии экстремистской деятельности» понятие «преступление экстремистской направленности» определено и в ч. 2 примечания к ст. 282.1 УК РФ, согласно которой под преступлениями экстремистской направленности понимаются преступления, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы, предусмотренные соответствующими статьями Особенной части Уголовного Кодекса и пунктом «е» ч. 1 ст. 63 УК РФ[59].

Однако в рамках данной работы изучению подлежит не вся экстремистская деятельность в целом, а лишь одно из возможных ее проявлений – экстремизм в социальных сетях, который, учитывая нормы действующего российского законодательства, может содержать признаки, как уголовного преступления, так и административного правонарушения. В частности, публичные призывы к осуществлению экстремистской деятельности с использованием сети «Интернет», согласно ч. 2 ст. 280 УК РФ, признаются уголовным преступлением[60], как и деяния, предусмотренные ч. 2 ст. 280.1 «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации» и ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» главы 29 Уголовного закона, а производствои распространение экстремистских материалов, пропаганда и публичное демонстрирование нацистской атрибутики или символики, а так же атрибутики или символики экстремистских организаций, в том числе с использованием информационно-коммуникационных технологий, рассматривается как административное правонарушение[61]. Между тем, согласно п. 8 Постановления Пленума Верховного Суда РФ от 28 июня 2011 г№ 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности», в случае, когда лицо распространяет экстремистские материалы, включенные в опубликованный федеральный список экстремистских материалов, с целью возбудить ненависть либо вражду, а также унизить достоинство человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, содеянное им должно влечь уголовную ответственность по ст. 282 УК РФ. Само понятие экстремистских материалов закреплено п. 3 ст. 1 Федерального закона от 25

[58] Макеева И.С. Экстремизм как уголовно-правовая категория // Законодательство и экономика. 2014. № 6. С. 61 - 68.
[59] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.11.2015) ч. 2 примечания ст. 282.1 // Собрание законодательства РФ.- 17 июня.- 1996.- № 25. Ст. 2954.
[60]Там же ч. 2 ст. 280.
[61]Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 14.12.2015) ст.ст. 20.29, 20.3 // Российская газета.- 31 декабря.- 2001.- № 256.

июля 2002 г № 114-ФЗ «О противодействии экстремистской деятельности». Согласно положениям указанной нормы экстремистские материалы это документы или информация на иных носителях, предназначенные для обнародования, призывающие к осуществлению экстремистской деятельности или обосновывающие, оправдывающие необходимость осуществления такой деятельности. К экстремистским материалам относятся и труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии, публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы. Необходимо отметить, что информационные материалы могут быть признаны экстремистскими только судом по месту их обнаружения на основании заявления прокурора или при производстве по соответствующему делу об административном правонарушении, гражданскому или уголовному делу[62]. Для отнесения материалов к экстремистским необходимо проведение судебной лингвистической экспертизы определение о проведении которой выносит суд. Результаты проведенной экспертизы оформляются заключением эксперта, отвечающем всем требованиям Федерального закона от 31 мая 2001 г № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». Обязательным признаком экстремистских материалов, как указал Конституционный Суд Российской Федерации в своем Определении от 02 июля 2013 г № 1053-О, является явное или завуалированное противоречие соответствующих действий (документов) конституционным запретам возбуждения ненависти и вражды, разжигания розни и пропаганды социального, расового, национального, религиозного или языкового превосходства, наличие которого должно определяться с учетом всех значимых обстоятельств каждого конкретного дела[63]. Что касается публичных призывов к экстремистской деятельности, то Постановление Пленума Верховного Суда РФ от 28 июня 2011 г№ 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» публичными призывами признает выраженные в любой форме обращения к другим лицам с целью побудить их к осуществлению экстремистской деятельности[64]. Важным признаком, в данном случае, является открытость, доступность призывов, их способность быть воспринимаемыми неопределенным кругом лиц. Следовательно, беседы в виртуальном пространстве, не рассчитанные на публичное обсуждение, ознакомление с информацией других лиц, т.е. личная переписка, публичными не являются и потому не могут влечь наступление юридической ответственности. Так же не является

[62] О противодействии экстремистской деятельности: Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 23.11.2015) ст. 13 // Российская газета.- 30 июля.- 2002.- 138-139.

[63] Об отказе в принятии к рассмотрению жалобы гражданина Кочемарова Владислава Сергеевича на нарушение его конституционных прав положениями пунктов 1 и 3 статьи 1 и части третьей статьи 13 Федерального закона «О противодействии экстремистской деятельности»: Определение Конституционного Суда РФ от 02.07.2013 N 1053-О // Вестник Конституционного Суда РФ.- 2014.- № 2.

[64] О судебной практике по уголовным делам о преступлениях экстремистской направленности: Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 п. 4 // Бюллетень Верховного Суда РФ.- август.- 2011.- № 8.

преступлением высказывание суждений и умозаключений, использующих факты межнациональных, межконфессиональных или иных социальных отношений, если они не преследовали цели возбудить ненависть либо вражду, а равно унизить достоинство человека либо группы лиц по дискриминационным признакам.

Современная действительность такова: наиболее популярные социальные сети – «ВКонтакте», «Фейсбук», «Инстаграм», «Одноклассники», «Твиттер» – изобилуют информацией экстремистского характера и призывами к экстремистской деятельности. По данным исследовательских компаний TNS и Brand Analytics лидерство по количеству зарегистрированных пользователей, посещаемости и публикуемых сообщений среди перечисленных сохраняет социальная сеть «ВКонтакте», 32,27% российской аудитории которой составляют пользователи в возрасте 18-24 лет (1 972185 пользователей); 32,06% - 25-34 лет (1 959009 пользователей); 24,05% - до 18 лет(1 469534 пользователей); 7,10% - 35-44 лет (433725 пользователей); 2,44% - 45-54 лет (148905 пользователей); 2,09% - 55 и старше (127918 пользователей)[65]. Популярность данной социальной сети объясняется, прежде всего, возможностью свободного обмена информацией, неограниченной коммуникации в реальном времени, консолидации в виртуальные социальные сообщества, в рамках которых происходит обсуждение наиболее актуальных общественных явлений и процессов. Как видно из приведенных выше показателей потенциальную аудиторию социальной сети составляет молодежь, на сознание которой и направлена информационная атака экстремистов.

Статистические данные, касающиеся зарегистрированных на территории России преступлений экстремисткой направленности, свидетельствуют о росте преступности в данном сегменте. Согласно опубликованной Министерством внутренних дел Российской Федерации «Краткой характеристике состояния преступности в РФ» количество преступлений экстремистской направленности, зарегистрированных на территории России, в январе – декабре 2013 г составило 896[66], за тот же период в 2014 г – 1024[67], в 2015 г – 1308[68]. При этом основной прирост достигнут за счет выявления преступлений, предусмотренных ст.ст. 280, 280.1, 282 УК РФ, совершаемых с использованием социальных интернет-сетей. В Алтайском крае, исходя из информационно-аналитических материалов, в 2013 году совершено 21 преступление экстремистской направленности, 7 из которых квалифицированы по ст. 281, 6 – по ст. 280 УК РФ[69]. В 2014 году общее количество совершенных

[65]BrandAnalytics: Статистика социальных сетей [Электронный ресурс]: Режим доступа: http://br-analytics.ru/statistics/author (дата обращения 18.01.2016).

[66]Краткая характеристика состояния преступности в Российской Федерации, в том числе в Крымском федеральном округе за январь - декабрь 2013 года. [Электронный ресурс]: Статистические сведения / Официальный сайт МВД РФ.: МВД РФ, 2014. - Режим доступа: https://mvd.ru/folder/101762/item/1609734/

[67]Там же - Режим доступа: https://mvd.ru/folder/101762/item/2994866/

[68]Там же - Режим доступа: https://mvd.ru/folder/101762/item/7087734/

[69] Информационно-аналитические материалы к отчету начальника Главного управления МВД России по Алтайскому краю генерал-лейтенанта полиции Торубарова Олега Ивановича перед депутатами Алтайского краевого Законодательного Собрания [Электронный ресурс]: Отчеты перед населением / Официальный сайт МВД РФ.: МВД РФ,2014.-Режим_доступа: https://22.mvd.ru/Dejatelnost/otchnas/Otcheti_za_2013_god/Otchet_nachalnika_Glavnogo_upravlenija_M

преступлений рассматриваемой категории составило 25. Из указанного числа 4 по ст. 280, 13 – по ст. 282 УК РФ[70]. Административная практика за 2013 – 2015 годы показала стремительный рост правонарушений в данной области. Согласно официальным данным за январь – декабрь 2013 года в Алтайском крае не было выявлено ни одного правонарушения, предусмотренного ст. 20.29 «Производство и распространение экстремистских материалов» КоАП РФ.В2014 году жителями Алтайского края было совершено 1 правонарушение указанной категории. А в 2015 году органами внутренних дел было зарегистрировано уже 7 правонарушений, квалифицируемых по ст. 20.29 КоАП РФ. Анализ уголовных дел и дел об административных правонарушений показал, что субъектами совершенных преступлений выступают лица в возрасте 20 - 24 лет, при этом больше всего правонарушений и преступлений совершенно именно пользователями «ВКонтакте». Несмотря на активное сотрудничество указанной социальной сети с органами внутренних дел в вопросе удаления экстремистских материалов, «ВКонтакте» изобилует группами, ведущими открытую пропаганду религиозного экстремизма и фундаментализма, национальной экстремистской деятельности. Оценивая официальную статистику, необходимо учитывать высокую латентность преступлений экстремистской направленности, совершенных с использованием социальных сетей, причем не только скрытую, но и скрываемую, когда мотивы таких деяний смешивают с хулиганскими либо иными побуждениями, что, безусловно, влияет на квалификацию деяния и существенно изменяет его юридическую оценку. Таким образом, можно предположить, что степень угрозы экстремизма гораздо выше, чем отражают статистические данные. Несмотря на то, что составы преступлений, предусмотренные ч. 2 ст. 280, ч. 2 ст. 280.1, ст. 282 УК РФ и правонарушений по ст.ст. 20.3, 20.29 КоАП РФ, представляют собой ненасильственные формы экстремистских проявлений, они зачастую являются побудительным мотивом к совершению насилия, нередко влекущего смерть потерпевших.

Резюмируя выше изложенное, можно говорить о том, что, во-первых, в настоящее время отсутствует единое общепризнанное теоретическое обоснование понятия «экстремистская деятельность», а закрепленное действующими нормативными правовыми актами определение не отличается точностью и однозначностью, что в совокупности допускает произвольный подход к его применению. Во-вторых, проявление экстремизма в социальных сетях по формам – это и текстовые сообщения, и графические изображения, и аудио-видео файлы – и способам – от распространения экстремистских материалов и публичных призывов к осуществлению экстремистской деятельности до попыток насильственного изменения основ конституционного строя – отличается разнообразностью, что, при отсутствии единого подхода к толкованию понятия и квалифицирующих признаков, значительно усложняет работу правоприменителя по профилактике экстремизма в социальных сетях и уголовно-правовой защите общества от крайне радикальных

[70]Там же -Режим_доступа:
https://22.mvd.ru/Dejatelnost/otchnas/Otcheti_za_2014_god/Otchet_nachalnika_Glavnogo_upravlenija_M

деяний. В-третьих, данные официальной статистики, представленные МВД России, свидетельствуют о ежегодном росте преступности экстремистского характера в целом, и экстремизма в социальных сетях в частности. При этом большинство преступлений экстремистской направленности совершенно пользователями «ВКонтакте», основную аудиторию которой составляет молодежь. В-четвертых, экстремисты активно используют сеть «Интернет» для: поиска и обмена информацией, создания сетей, координации деятельности, вербовки, поиска способов финансирования. Учитывая изложенные цели, а так же масштабы противоправной деятельности экстремистов можно говорить о возникновении нового негативного явления – «киберэкстремизма», способного дестабилизировать любое развитое государство. Поэтому неслучайно в Стратегии национальной безопасности Российской Федерации в числе основных источников угроз национальной безопасности указывается на деятельность террористических и экстремистских организаций[71].

Причины и условия экстремизма в социальных сетях. Обострение экстремистских проявлений в социальных сетях, основными субъектами которых выступают молодые люди, обуславливает необходимость изучения комплекса причин и условий, способствующих совершению преступлений, предусмотренных ч. 2 ст. 280, ч. 2 ст. 280.1, ст. 280 УК РФ, и правонарушений, закрепленных ст.ст. 20.3, 20.29 КоАП РФ. Поскольку рассматриваемое негативное явление отличаетсяот других проявлений экстремизма одновременно субъектом – в основной массе молодежь, и специфическим способом совершения – использование социальной интернет-сети, постольку проблемой экстремизма в социальных сетях заинтересовались ученые из разных отраслей: социологии, политологии, педагогики, философии, и, разумеется, юриспруденции.

Возникновение экстремизма в России исследователи, прежде всего, связывают с социально-политическими и социально-экономическими причинами. По мнению ряда специалистов, именно смена политического и экономического строя спровоцировала нестабильность общественных отношений. Спад экономики, снижение производства привели к сокращению рабочих мест, обнищанию населения, что в совокупности породило многонациональную армию безработных, лишенных элементарных условий для физического выживания. А.В. Петрянин обращает внимание на то, что значительная масса населения – 46,2%, относит себя к малоимущим слоям,что является одной из причин экстремистских настроений населения, особенно у молодой его части[72].Снижение уровня жизни населения, постоянно увеличивающийся разрыв между богатыми и бедными, как следствие, ведут к нарастанию социальной напряженности в российском обществе. Как утверждают А.В. Смагина Д.И. Сопун в статье «Причины распространения экстремизма в России», маргинальные слои населения из-за личных неурядиц утрачивают чувство терпимости и озабочены

[71] О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31.12.2015 п. 43 // Собрание законодательства РФ.- 04 января.- 2016.- № 1 (часть II). Ст. 212.

[72] Петрянин А.В. Противодействие преступлениям экстремистской направленности: уголовно-правовой и криминологический аспекты. М., 2014. С. 329.

поиском врага. В подтверждение сказанного специалисты приводят результаты совместного исследования Института социологии РАН и российского отделения германского Фонда имени Ф. Эберта «Двадцать лет реформ глазами россиян», согласно которым: 76% респондентов из числа россиян считают, что двадцать лет политических и экономических реформ в России не принесли им главного богатства - свободы. Кроме того, за последние десять лет агрессия резко возросла. Утверждается, что 34% россиян постоянно испытывают желание «перестрелять всех взяточников и спекулянтов», а 38% «иногда» испытывают такое желание[73]. Кроме указанных выше к экономическим детерминантам экстремизма в социальных сетях относят: усиление имущественного неравенства; замедление темпов формирования среднего слоя, который в состоянии обеспечить социальную стабильность в обществе; расширение криминальных кругов за счет числа маргинализированных и люмпенизированных людей.

Немаловажное влияние на развитие экстремизма в социальных сетях оказывает неконтролируемый процесс миграции. Пользователи сети «Интернет», создавая сообщества и наполняя их негативной информацией экстремистского характера, например «скажем НЕТ мигрантам!», «Россия для Русских!» (открытые группы социальной сети «ВКонтакте») и т.д., выражают свое недовольство отсутствием эффективной государственной миграционной политики, а так же непринятием действенных мер по прекращению притока населения из стран ближнего зарубежья. Кроме того проблемная социальная адаптация и интеграция мигрантов на новой территории пребывания, этнокультурные и этнопсихологические различия влекут за собой межэтническую разобщенность, дискриминацию по национальному признаку, вероисповеданию, языку, что проявляется путем размещения «недовольными» негативного контента на своих страницах в социальных сетях. Как правило, группы, направленные на дискредитацию определенного этноса, имеют двойного адресата: «своих» - тех кто разделяет неприязнь; и «чужих» - защитников дискредитируемой группы. При этом активная полемика на стене группы и в обсуждениях (темах) ведется именно между «своими» и «чужими». Коммуникация внутри подобной виртуальной группы отличается вербальной (речевой) агрессией, для которой характерно словесное выражение негативных эмоций, чувств или намерений в оскорбительной, грубой форме. Речевая агрессия, в данном случае, выражает целенаправленное желание говорящего нанести коммуникативный урон адресату, например, унизить, оскорбить, высмеять и т. п. По мнению экспертов, в России утрачен контроль над миграционными потоками. Причины тому, во-первых, открытость границ России со странами СНГ, а во-вторых, нелегальное проживание и неофициальное трудоустройство лиц, приезжающих из постсоветского пространства[74]. Мигранты участвуют в распределении и потреблении социальных

[73]Смагина А.В., Сопун Д.И. Причины распространения экстремизма в России // Российский следователь. 2012. № 8. С. 33 - 36.
[74] Смагина А.В., Сопун Д.И. Причины распространения экстремизма в России // Российский следователь. 2012. № 8. С. 33 - 36.

ресурсов что, в условиях экономического кризиса, вызывает явно негативную реакцию со стороны населения страны, особенно молодежи.

Экспрессивное публичное выражение недовольства молодежью, проявляемое в социальных сетях, объясняется, прежде всего, особенностями социального положения, психологическими свойствами указанной возрастной группы. Именно в молодом возрасте несовершенство окружающего социального мира ощущается наиболее остро .Соответственно, появляется либо желание отгородиться от этой действительности и создать свой собственный мир (вариант «ухода»), либо его переделать (вариант «мятежа»)[75]. Следовательно, в качестве детерминантов экстремизма в социальных сетях можно назвать социально-психологические и социально-возрастные особенности основных субъектов преступлений изучаемой категории. Экстремальное сознание, переходный, неустоявшийся, во многом маргинальный социальный статус, а так же несформированность политического, экономического, религиозного сознания у молодых людей ведут к тому, что они легко подвергаются внушению и манипулированию, чем своевременно пользуются экстремисты. Кроме того, достижению противоправных целей экстремистов способствует нарастающее вмешательство западной инородной культуры в традиционное российское пространство, в результате которого происходит деформация мировоззрения у части молодежи. Обострение ситуации происходит в связи с отсутствием у современных молодых людей позитивных образцов самореализации, что в совокупности с социально-экономической нестабильностью, негативным воздействием средств массовой информации, деструктивными социокультурными явлениями, общей криминализацией общества ставит молодежь в сложные условия выбора основ жизнедеятельности и способствует формированию экстремистских проявлений в социальных сетях[76].

Указанные выше детерминанты тесно связаны с отсутствием реальной, а не показной молодежной политики государства. Проблемное состояние института семьи и брака в нашей стране не позволяет обеспечить детей и молодых людей достойной социализацией и адекватным воспроизведением социальных норм и запретов, результатом же данных процессов является формирование у молодых людей агрессивного поведения[77]. В тоже время радикальные исламисты считают работу в молодежной среде одним из главных, приоритетных направлений своей деятельности, что, учитывая широкомасштабную экспансию радикального ислама, создает реальную угрозу национальной безопасности страны.

В числе причин распространения экстремизма в социальных сетях необходимо указать специфику их функционирования, позволяющую участникам не только общаться в режиме реального времени через любые границы, размещать любую информацию на досках объявлений, загружать данные из любых ресурсов и т.д., но и

[75] Реутов Е. В. Причины распространения экстремизма и ксенофобии в молодежной среде. Белгород, 2008. С. 74.
[76]Лелеков В.А., Черных А.А. О причинах преступлений экстремистской направленности в молодежной среде // Российский следователь. 2015. № 8. С. 42 - 46.
[77]Там же.

получать информацию, которая недоступна через официальные средства массовой информации, для обхода цензуры, блокировки и т.п. Большинство социальных сетей запрещают анонимность пользователей и предусматривают обязательную регистрацию, однако не гарантируют, что сведения, указанные участником являются достоверными. Таким образом, в интернет-сообществе у человека создается виртуальная личность, которая нередко отличается от его реальной, и может быть даже важнее последней. Кроме того, виртуальные сообщества, создаваемые в социальных сетях, благодаря анонимности коммуникации в «Интернете», снимают географические и психологические барьеры в общении, что способствует росту экстремизма, поскольку пользователь не чувствует персональную ответственность за действия, совершаемые им в социальной сети – считает себя безнаказанным. Так же необходимо отметить технические свойства социальных сетей, способствующие распространению экстремизма, в частности возможность регистрировать доменные имена сайта на одной территории (в одной стране), а размещать информацию на другой. Н.А. Морозова в статье «Проблемы привлечения к уголовной ответственности за экстремизм в информационной сети Интернет» отмечает, что: «При размещении материалов, направленных на возбуждение ненависти или вражды, а равно на унижение человеческого достоинства посредством сети Интернет, вполне возможна ситуация, что интернет-провайдер находится в одном месте, владелец ресурса - в другом, пользователь социальной сети - в третьем, а свой профиль он зарегистрировал в четвертом. Комментарии и обсуждение ведутся из разных мест по территориальной принадлежности, в т.ч. и самим пользователем, зарегистрировавшим профиль. В данном случае определить место совершения преступления будет практически невозможно.»[78]. Данный вывод исследователя подтверждается, с нашей точки зрения, и тем, что виртуальная сеть позволяет публиковать запрещенную информацию не только с персонального устройства, имеющего свой IP-адрес, но и через систему предоставления доступа в «Интернет»-маршрутизаторы - в кафе, гостиницах, аэропортах и т.п., что не дает технической возможности определить место совершения преступления.

В качестве детерминантов экстремизма в социальных сетях следует выделить и несовершенство правоприменительной практики в отношении рассматриваемых действий. Экстремизм, как социальное явление, на сегодняшний день, характеризируется сложностью, многоплановостью и фактическим отсутствием точных границ, в связи с чем, правовая квалификация и доказывание преступлений, предусмотренных ст. ст. 280, 280.1, 282 УК РФ вызывает у следственных органов значительные трудности. Логическим следствием указанных обстоятельств, а также новизны и несовершенства антиэкстремистского законодательства в целом выступает трудно разрешаемая коллизия составов преступлений экстремистской направленности. Учитывая разъяснения данные Верховным Судом РФ в п. 4, 7 Постановления Пленума Верховного Суда РФ от 28 июня 2011 № 11 «О судебной

[78] Морозова Н.А. Проблемы привлечения к уголовной ответственности за экстремизм в информационной сети Интернет // Российский следователь. 2014. № 5. С. 38 - 41.

практике по уголовным делам о преступлениях экстремистской направленности», следует отметить, что публичные призывы к нарушению прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии сами по себе возбуждают ненависть и вражду по указанным признакам. В то же время формой возбуждения ненависти либо вражды является призыв к экстремистской деятельности. Таким образом, составы преступлений, предусмотренные ч. 2 ст. 280 и ч. 1 ст. 282 УК РФ, в рассматриваемой части совпадают по основным объективным и субъективным признакам, в том числе описанию признаков деяния, а поэтому в ситуации конкретного уголовного дела не могут быть вменены в вину одновременно[79]. К сожалению, в правоприменительной практике такие случаи не является редкостью, хотя подобная правовая оценка деяний противоречит нормам Основного и Уголовного законов, а именно: ч. 1 ст. 50 Конституции РФ, ч. 2 ст. 6 УК РФ. Рассматриваемая правовая ситуация, в силу устоявшегося правила разрешения конкуренции специальных норм Особенной части УК РФ, требует применения только одной из специальных норм - нормы более специальной, т.е. наиболее точно описывающей признаки совершенного деяния, наиболее полно охватывающей все его обстоятельства[80]. Поэтому при наличии в одном деянии признаков составов ст. 280 и ст. 282 УК РФ следует оценивать по правилам разрешения конкуренции специальных норм и квалифицировать содеянное по ст. 282 УК РФ, при наличии иных признаков этого состава преступления. Соотношение же норм ст. ст. 280 и 280.1 УК РФ необходимо характеризовать, согласно официальному отзыву Верховного Суда РФ, как конкуренцию общей и специальной норм и применять при установлении в деянии лица признаков обеих состав ст. 280.1 УК РФ[81]. Неправильная квалификация деяний ведет к тому, что лица ошибочно привлекаются к уголовной ответственности по статье, предусматривающей более мягкое наказание, либо не привлекаютсяк ответственности вообще. Кроме собственно правовой оценки деяний наибольшие затруднения вызывает установление умысла на возбуждение ненависти или вражды, а равно унижение чести и человеческого достоинства.Анализ материалов уголовных дел и материалов, по которым в возбуждении уголовного дела отказано, дает основание констатировать, что большинство обвиняемых на допросах отрицают наличие цели возбуждения ненависти или вражды, оскорбления по национальному и иному признаку, они только высказывали свое мнение, делились точкой зрения. Подобное положение зачастую приводит к тому, что органы следствия прекращают или отказывают в возбуждении уголовного дела в связи с отсутствием состава

[79] Степанов В.В., Струков А.В. Проблемы разрешения конкуренции составов преступлений экстремистской направленности // Вестник Пермского университета. Юридические науки. 2015. № 1. С. 133 - 140.
[80] Там же.
[81] Официальный отзыв Верховного Суда РФ от 27.11.2013 № 2-ВС-5196/13 «На проект Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации в целях установления ответственности за публичные призывы к действиям, направленным на нарушение территориальной целостности Российской Федерации» // СПС. «КонсультантПлюс». 2015.

преступления[82]. Безнаказанность, равно как и мягкость наказания, в таких случаях еще больше уверяет субъектов в своей «правоте», создает предпосылки для дальнейшего распространения идей экстремизма в социальных сетях.

Значительное влияние на рост преступности в изучаемом сегменте оказывают и, возникающие в практике следователей, проблемы привлечения к уголовной ответственности лиц за размещение материалов, содержащих признаки экстремизма, на форумах, особенно в закрытых группах. Такие факты в ряде случаев не признаются публичным распространением, в связи с чем в возбуждении уголовных дел отказывают[83]. Кроме того для документирования выявленных в ходе мониторинга интернет-сайтов признаков экстремистской деятельности, необходимо точное доказывание умысла на совершение уголовно-наказуемого деяния. С этой целью проводятся психолингвистические исследования и экспертизы, достоверно устанавливающие в исследуемых материалах признаки экстремистской деятельности. Однако специалисты-эксперты подобного профиля в большинстве экспертных подразделениях системы МВД отсутствуют или их квалификация не отвечает требованиям, предъявляемым органами предварительного следствия и судом[84]. На практике длительное и некачественное проведение экспертиз приводит к утрате возможности получения доказательств экстремистской деятельности и, как следствие, эффективного расследования преступлений экстремистской направленности в социальных сетях .В то же время, проведение подобных исследований и экспертиз в частных экспертных организациях связано со значительными материальными затратами. Так же в настоящее время широко распространены ситуации, когда по одному и тому же информационному материалу имеются экспертные заключения с противоположными выводами. Причем оба заключения могут содержать немотивированные оценочные суждения и предположения о возможном понимании или вероятном воздействии текста на абстрактного адресата[85]. Однако следует учитывать следующее: заключение эксперта не является окончательным доказательством по делу, оно не имеет заранее установленного доказательственного значения. Выводы экспертизы суд должен будет исследовать наряду с другими доказательствами, собранными в ходе предварительного расследования уголовного дела либо представленными сторонами при рассмотрении гражданского дела.

Изложенное позволяет нам говорить о том, что детерминанты экстремизма в социальных сетях весьма многообразны и охватывают практически все важнейшие сферы жизнедеятельности современного общества. Условно все перечисленные причины и условия можно разделить на общие и специальные. При этом общие детерминанты обуславливают развитие экстремизма в стране в целом как негативного

[82] Морозова Н.А. Проблемы привлечения к уголовной ответственности за экстремизм в информационной сети Интернет // Российский следователь. 2014. № 5. С. 38 - 41.
[83] Там же.
[84]Бедарев К.В. Противодействие преступлениям, совершаемым по мотивам расовой, национальной или религиозной ненависти или вражды в сети Интернет. Краснодар. 2015. С. 110.
[85] Кузнецов С.А., Оленников С.М. Экспертные исследования по делам о признании информационных материалов экстремистскими: теоретические основания и методическое руководство (научно-практическое издание). М., 2014. С. 133.

социального явления. Специальные же причины и условия объясняют рост экстремизма в социальных сетях. К первой группе относятся: обще-социальные, социально-экономические, социально-политические, идеологические детерминанты. В частности общими причинами и условиями можно назвать: спад экономического развития; растущая безработица; снижение уровня жизни населения; усиление имущественного неравенства и расслоения; кризис современного общества; проблемы института семьи и брака; экстремальное, несформированное сознание основных субъектов рассматриваемой категории преступлений - молодых людей; отсутствие позитивных образов самореализации; негативное воздействие средств массовой информации; деструктивные социально-культурные явления; отсутствие эффективной государственной молодежной и миграционной политики. Вторую группу составляют детерминанты, напрямую связанные с особенностями функционирования социальных сетей и проблемами правоприменительной практики. К ним относятся: открытый доступ к социальным сетям; экстерриториальность и анонимность общения в сети «Интернет», что позволяет общаться в режиме реального времени через любые границы, размещать любую информацию на досках объявлений, загружать данные из любых ресурсов, получать информацию, которая недоступна через официальные средства массовой информации, для обхода цензуры, блокировки; возможность регистрировать доменные имена сайта на одной территории, а размещать информацию на другой, используя при этом различные технические средства; латентность преступлений изучаемой направленности; относительная редкость и «точечный характер» их проявлений; особая сложность в расследовании дел, в частности, при правовой квалификации, доказывании, установлении личности лица, совершившего инкриминируемое преступление (идентификация «виртуальной личности» с реальным субъектом конкретного правоотношения), его вины, а так же признании, размещенных этим лицом материалов экстремистскими.

Профилактика экстремизма в социальных сетях. Экстремизм в социальных сетях является одной из наиболее сложных проблем современного российского общества. Как негативное социально-правовое явление он оказывает дестабилизирующее влияние на социально-политическую обстановку в стране и угрожает национальной безопасности Российской Федерации. В этой связи одним из приоритетных направлений национальной правовой политики является создание эффективного механизма профилактики преступлений изучаемой направленности. Логичным представляется, что, в рамках противодействия экстремистской деятельности, одной из главных задач федеральных органов власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, правозащитных организаций является осуществление, в пределах своей компетенции, не только профилактических, но и воспитательных, пропагандистских, мер, направленных на предупреждение экстремистской деятельности.

Вопрос о степени участия государства и воздействия правового регулирования на развитие сети «Интернет» вообще и социальных сетей в частности является дискуссионным и активно исследуется в настоящее время. Как утверждает группа авторов статьи «Социальные интернет-сети: правовые аспекты» С.А. Перчаткина, М.Е. Черемисинова, А.М. Цирин, М.А. Цирина, Ф.В. Цомартова: «Социальные интернет-сети задумывались как самоорганизующиеся и саморегулируемые сообщества, а попытки установить любые дополнительные ограничения влекут негативную реакцию и сильный общественный резонанс со стороны интернет-сообщества.»[86].С резкой критикой положений о внесудебной блокировке веб-ресурсов выступили крупные интернет-сервисы, например «Официальный блог Google Россия», «Российская ассоциация электронных коммуникаций», активисты «Пиратской Партии России». Что касается саморегулирования социальных сетей, то данный процесс осуществляется путем модерации и администрирования. Указанные меры призваны обеспечить порядок на форуме, возможность редактировать и удалять любые темы и отдельные сообщения в группе для того, чтобы поддерживать дискуссию в рамках этических норм. Модератор или администрация могут закрыть какую-либо тему (удалить ее), если считают, что ее дальнейшее развитие может повлечь нежелательные или опасные последствия, однако решение о наложении запрета на тему или об удалении информации остается на усмотрение конкретных лиц администрации ресурса[87]. Таким образом, учитывая важность обеспечения государственных интересов и поддержки развития механизмов саморегулирования внутри интернет-сообщества, целесообразно определить характер и меру регулирования распространения информации через социальные сети и контроля над виртуальным пространством со стороны государства в лице его органов власти.

Согласно действующему российскому законодательству передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации. В тоже время, передача информации может быть ограничена, но только в порядке и на условиях, которые установлены федеральными законами[88]. Порядок ограничения доступа к информации, содержащей призывы к осуществлению экстремистской деятельности в сети «Интернет», регламентирован ст. 15.3 Федерального закона от 27 июля 2006 г № 149-ФЗ «Об информации, информационных технологиях и о защите информации».Так в случае обнаружения в сети «Интернет» противоправного контента Генеральный прокурор Российской Федерации или его заместители направляют требование в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой

[86] Перчаткина С.А., Черемисинова М.Е., Цирин А.М., Цирина М.А., Цомартова Ф.В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2012. № 5. С. 14 - 24.
[87]Перчаткина С.А., Черемисинова М.Е., Цирин А.М., Цирина М.А., Цомартова Ф.В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2012. № 5. С. 14 - 24.
[88] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 13.07.2015) п. 5 ст. 15 // Российская газета.- 29 июля.- 2006.- № 165.

информации, массовых коммуникаций, информационных технологий и связи (далее Роскомнадзор), о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию. После чего Роскомнадзор незамедлительно реагирует на поступившее обращение, а именно:

- направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу, в том числе к сайту в сети «Интернет», или к информации, размещенной на нем и содержащей призывы к осуществлению экстремистской деятельности. Данное требование должно содержать доменное имя сайта в сети «Интернет», сетевой адрес, указатели страниц сайта, позволяющие идентифицировать такую информацию;

- определяет провайдера хостинга или иное лицо, обеспечивающее размещение в сети «Интернет», указанного информационного ресурса, и владельца сайта, на котором размещена негативная информация;

- направляет провайдеру хостинга (или иному лицу) уведомление в электронном виде на русском и английском языках о нарушении порядка распространения информации с указанием доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети «Интернет», на котором размещена информация, содержащая призывы к осуществлению экстремистской деятельности, а также указателей страниц сайта, позволяющих идентифицировать такую информацию, и требование принять меры по удалению противоправного контента;

- фиксирует дату и время направления уведомления провайдеру хостинга (или иному указанному лицу) в соответствующей информационной системе[89].

После получения требования Роскомнадзора оператор связи, оказывающий услуги по предоставлению доступа к сети «Интернет», обязан незамедлительно ограничить доступ к информационному ресурсу или к информации, размещенной на нем. Так же в обязанности провайдера входит в течение суток проинформировать обслуживаемого ими владельца информационного ресурса о получении подобного уведомления и о необходимости незамедлительно удалить запрещенную информацию. В случае если владелец информационного ресурса удалил информацию, содержащую призывы к осуществлению экстремистской деятельности, он направляет, в письменном или электронном виде, уведомление об этом в Роскомнадзор. В свою очередь Роскомнадзор проверяет достоверность этой информации и, при положительном результате, уведомляет по системе взаимодействия оператора связи о возобновлении доступа к информационному ресурсу.

Кроме приведенного выше закона использование сетей связи общего пользования для осуществления экстремистской деятельности равно как и распространение экстремистских материалов, их производство или хранение в целях распространения запрещено Федеральным законом от 25 июля 2002 г № 114-ФЗ «О

[89] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 13.07.2015) ч. 2 ст. 15.3 // Российская газета.- 29 июля.- 2006.- № 165.

противодействии экстремистской деятельности»[90]. В силу ст. 13 данного нормативного правового акта материалы признаются экстремистскими федеральным судом по месту их обнаружения, распространения или нахождения организации, осуществившей производство таких материалов, на основании представления прокурора или при производстве по соответствующему делу об административном правонарушении, гражданскому или уголовному делу. В дальнейшем, в соответствии с пп. 30.28 п. 7 Положения о Министерстве юстиции Российской Федерации (далее Минюст РФ), утвержденного Указом Президента РФ от 13 октября 2004 г № 1313, Минюст РФ определяет порядок ведения, ведет и публикует на своем официальном сайте федеральный список экстремистских материалов[91]. На сегодняшний день указанный список содержит 3258 позиций[92]. Следует отметить, что в последние годы экстремисты стали размещать множество аудиофайлов и видеороликов. Проведя анализ федерального списка, можно утверждать, что более 700 из общего числа позиций представляют собой ссылки на страницы пользователей «ВКонтакте», на которых размещались экстремистские материалы. Вместе с тем, учитывая положения Определения Верховного Суда РФ от 10 мая 2011 г№ 58-Впр11-2,операторы связи, предоставляющие телекоммуникационные услуги доступа к информационной сети «Интернет», имеют техническую возможность ограничения доступа к экстремистским материалам путем фильтрации трафика и полного блокирования доступа к IP-адресу сайта или отдельной странице сайта, на которой размещен материал (аудио, видеофайл, печатный текст)[93]. Однако, несмотря на вышеизложенное, негативные тенденции в динамике преступлений экстремистской направленности, совершаемых в социальных сетях, в настоящее время продолжают иметь место. Свои рекомендации по решению данного вопроса высказывают ряд исследователей данной области, в частности Н.Н. Телешина предлагает: ужесточить ответственность за распространение экстремистской информации через сайты социальных сетей в «Интернете»; внести в законодательство изменения, согласно которым провайдеры интернет-связи и сотовые операторы привлекались бы к субсидиарной ответственности за правонарушения, совершенные их клиентами в виртуальном пространстве; принять федеральный закон «Об электронном документе», положения которого регулировали бы информационные отношения в виртуальном пространстве; ввести обязательную контентную фильтрацию сайтов сети «Интернет» в учреждениях системы образования с целью охраны психического

---

[90] О противодействии экстремистской деятельности: Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 23.11.2015) ст.ст. 12, 13 // Российская газета.- 30 июля.- 2002.- 138-139.

[91] Положения о Министерстве юстиции Российской Федерации: утв. Указом Президента РФ от 13.10.2004 N 1313 (ред. от 31.12.2015) пп. 30.28 п. 7 // Российская газета.- 19 октября.- 2004.- № 230.

[92] Федеральный список экстремистских материалов [Электронный ресурс]: Федеральный список экстремистских материалов / Официальный сайт Минюст России.: Минюст РФ, 2016. - Режим доступа: http://minjust.ru/ru/extremist-materials?field_extremist_content_value= (дата обращения 02.02.2016)

[93]Дело об ограничении доступа к Интернет-сайту направлено на новое рассмотрение в суд первой инстанции, так как суд не учел, что предоставляя техническую возможность доступа к запрещенной законом информации, ответчик фактически выступает ее распространителем в отношении других лиц, имея техническую возможность, он должен в силу закона принять меры по ограничению доступа к Интернет-сайту: Определение Верховного Суда РФ от 10.05.2011 N 58-Впр11-2 // Бюллетень Верховного Суда РФ.- 2011.- № 12.

здоровья несовершеннолетних; улучшить координацию правоохранительных органов и субъектов гражданского общества в области контроля виртуального пространства; усовершенствовать программы и механизмы подготовки специалистов в области информационной безопасности[94]. Реализация указанных выше мероприятий, бесспорно, позволила бы более эффективно бороться с преступностью в изучаемом сегменте. Вместе с тем необходимо отметить, что профилактика экстремистской деятельности может быть признана успешной лишь при системном подходе субъектов такой профилактики: органов власти, правоохранительных органов, антитеррористических комиссий, заинтересованных министерств и ведомств и органов местного самоуправления. При этом акцент необходимо делать не столько на репрессивные, сколько на воспитательные, пропагандистские меры, направленные на предупреждение экстремистской деятельности. Для этого целесообразно использовать потенциал общественных, научных и религиозных объединений, других институтов гражданского общества. Необходимо активно развивать уже имеющиеся и создавать новые формы взаимодействия всех субъектов профилактики экстремизма в сети «Интернет».

Бесспорным остается тот факт, что правоохранительные органы, в широком смысле этого слова, играют важнейшую роль в профилактике преступлений экстремистской направленности, совершаемых в социальных сетях. Данные органы, в отличие от субъектов «общей профилактики» - органов государственной власти, местного самоуправления, общественных организаций, образовательных учреждений, осуществляют целенаправленную деятельность по противодействию экстремизму, следовательно, являются основными участниками «специальной профилактики» изучаемого негативного явления. Ведущая роль в данной деятельности отведена структурным подразделениям органов внутренних дел.

В целях повышения эффективности и результативности в области противодействия экстремизму, комплексного использования в этой деятельности сил и средств органов внутренних дел Российской Федерации практически на все подразделения МВД России возложены определенные обязанности в пределах их компетенции. Специализированными структурами данной области являются: Главное управление по противодействию экстремизму МВД России (ГУПЭ МВД России) – самостоятельное структурное подразделение полиции, осуществляющее функции по выработке и реализации государственной политики и нормативному правовому регулированию, а также правоприменительные полномочия в области противодействия экстремистской деятельности и терроризму[95]; Управление «К» – подразделение МВД России, осуществляющее борьбу с преступлениями в сфере

[94]Телешина Н.Н. К вопросу о совершенствовании государственного контроля виртуального пространства // Информационное право. 2012. N 1. С. 25 - 30.

[95] Главное управление по противодействию экстремизму [Электронный ресурс] // Главное управление по противодействию экстремизму / Официальный сайт МВД России.: МВД РФ, 2016. - Режим доступа: https://mvd.ru/mvd/structure1/Glavnie_upravlenija/Glavnoe_upravlenie_po_protivodejstviju_j

информационных технологий[96]; Центр по противодействию экстремизму – подразделение ГУ МВД России осуществляющее выявление, предупреждение, пресечение и раскрытие преступлений террористического характера, преступлений и правонарушений экстремистской направленности, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших. В качестве правоохранительных органов «общего профиля» так же осуществляющих выявление, предупреждение и пресечение экстремисткой деятельности, в том числе и в сети «Интернет»,выступают органы прокуратуры. Их задачей в изучаемом сегменте является принятие мер по повышению действенности надзора за исполнением законодательства о противодействии использованию средств массовой информации для осуществления экстремистской деятельности, разжигания межнациональной розни. Прокуратурой регулярно проводятся проверки исполнения антиэкстремистского законодательства в деятельности средств массовой информации, а также в организациях, осуществляющих издательскую деятельность. Важнейшим направлением профилактики экстремизма выступает планомерная работа по предъявлению заявлений в суд о признании информационных материалов экстремистскими. Данная сфера правоохранительной деятельности осуществляется сотрудниками отдела по надзору за исполнением законов о федеральной безопасности, межнациональных отношениях, противодействии экстремизму и терроризму. Особое внимание уделяется наиболее посещаемым ресурсам: «ВКонтакте», «Твиттер» и т.д. Так же свой вклад в профилактику преступлений экстремисткой направленности в сети «Интернет» вносят: ГУУР МВД России - оказывает содействие подразделениям по противодействию экстремизму и организации деятельности по выявлению преступлений и правонарушений экстремистской направленности; ГУЭБ и ПК МВД России - оказывает содействие в проведение комплексных мероприятий по проверке и пресечению деятельности лиц и организаций, в отношении которых имеется информация о причастности к финансированию экстремистской деятельности и терроризма; ГУОООП МВД России, в пределах своей компетенции, участвует в профилактике и пресечении преступлений и правонарушений экстремисткой направленности в жилом секторе, на улицах, площадях, стадионах, в скверах, парках и др. общественных местах; принимает участие во взаимодействии с подразделениями по противодействию экстремизму, в организации профилактики преступлений и правонарушений экстремистской направленности; осуществляет в пределах компетенции меры, направленные на совершенствование работы подразделений по охране общественного порядка территориальных органов МВД России по профилактике преступлений и правонарушений экстремистской направленности; осуществляет взаимодействие с органами исполнительной власти субъектов Российской Федерации и органами местного самоуправления по вопросам совершенствования деятельности

[96] Управление «К» МВД России [Электронный ресурс] // Управление «К» МВД России / Официальный сайт МВД России.: МВД РФ, 2016. - Режим доступа: https://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii

территориальных органов МВД России по профилактике преступлений и правонарушений экстремистской направленности; обеспечивает в установленном порядке обмен имеющейся информацией, связанной с совершением преступлений и правонарушений экстремистской направленности, с подразделениями по противодействию экстремизму. В частности, входящие в структуру ГУОООП МВД России подразделения по делам несовершеннолетних, участковые уполномоченные полиции, сотрудники патрульно-постовой службы активно взаимодействуют с органами государственной власти по реализации поставленных перед ними задач по предупреждению экстремизма. Значительный роль в борьбе с экстремизмом в сети «Интернет» играют и подразделения территориальных органов внутренних дел, в частности: отдел уголовного розыска, дознания, следствия, дежурной части.

Указанные службы в своей деятельности руководствуются не только выше перечисленными нормативными правовыми актами, но ведомственными приказами, а так же должностными инструкциями. Основным документом, определяющим направления, формы и методы предупреждения преступлений, осуществляемые органами внутренних дел в пределах полномочий, предоставленных им законодательством Российской Федерации, является Приказ Министерства внутренних дел Российской Федерации от 17 января 2006 г № 19 «О деятельности органов внутренних дел по предупреждению преступлений» (вместе с «Инструкцией о деятельности органов внутренних дел по предупреждению преступлений»).Согласно п. 17 Приказа обязанности сотрудников подразделений по противодействию экстремизму включают: проведение мониторинга оперативной обстановки в области противодействия экстремистской деятельности; принятие мер по разобщению экстремистских организаций (сообществ) на ранних стадиях формирования путем поиска и своевременной реализации информации упреждающего характера; осуществление оперативно-розыскных мероприятий по предупреждению преступлений, отнесенных к компетенции подразделений по противодействию экстремизму, а так же осуществление мероприятий по недопущению проникновения представителей экстремистских организаций (сообществ) в органы государственной власти; участие в правовой пропаганде и информировании населения о результатах работы в установленной области деятельности; разработку и организацию проведения специальных операций и оперативно-профилактических мероприятий в установленной области деятельности; выявление при проведении оперативно-розыскных мероприятий причин и условий, способствующих совершению преступлений и принятие мер по их устранению[97].

На сегодняшний день у правоохранительных органов возникают трудности с правовыми основаниями проведения оперативно-розыскных мероприятий в сети «Интернет». Сотрудник оперативного подразделения, осуществляя мониторинг социальных сетей, инициативно выявляет латентные преступления экстремистской направленности и вынужден проводить оперативно-розыскные мероприятия. Однако,

[97] О деятельности органов внутренних дел по предупреждению преступлений: Приказ МВД России от 17.01.2006 № 19 (ред. от 30.12.2011) п. 17 // СПС. КонсультантПлюс. 2015.

следует учитывать, что на первоначальном этапе основания для проведения мероприятий, предусмотренные ст. 7 Федерального закона от 12 августа 1995 г № 144-ФЗ «Об оперативно-розыскной деятельности», могут отсутствовать. Изложенное позволяет говорить о наличии значительных пробелов по противодействию экстремизму в сети «Интернет» и необходимости внесения соответствующих дополнений в федеральное законодательство.

Результаты анализа правовой основы показывают, что имеющиеся в арсенале органов внутренних дел меры противодействия преступлениям экстремистской направленности не достаточно учитывают специфику противоправных действий в виртуальном пространстве. Полагаем, что, несмотря на фильтрацию и блокировку сайтов, содержащих информационные материалы экстремистского характера, они должны внимательно изучаться сотрудниками правоохранительных органов и спецслужб для выявления источников и каналов финансирования экстремизма, изучения и составления криминологических портретов лидеров, непримиримых и активных участников международных экстремистских организаций, структуры организованных преступных формирований, способов связи и конспирации, интенсивности посещаемости этих сайтов пользователями, участия в форумах. Однако, как отмечает К.В. Бедарев, большинство сотрудников органов внутренних дел оценивают свою подготовленность к работе в рассматриваемом направлении не соответствующей в полном объеме предъявляемым требованиям[98]. На практике сотрудникам подразделений по противодействию экстремизму в целях выполнения возложенных на них задач необходим широкий спектр специальных познаний, в том числе компьютерная грамотность, знание психологии, познания в области религии, владение полным объемом информации о деятельности различных экстремистских организаций и т.д. Поэтому вполне логичным представляется предложение о разработке специальных программ обучения, позволяющих формировать комплекс профессиональных умений и навыков по выявлению и документированию экстремистских проявлений в социальных сетях.

Необходимым условием эффективного противодействия экстремизму в социальных сетях является и международное сотрудничество в изучаемом сегменте. Глобальная информатизация общества не повышает, а понижает степень его безопасности. Современный «киберэкстремизм» способен вызвать системный кризис в любом государстве с высокоразвитой информационной инфраструктурой. В этих условиях уязвимость критических инфраструктур перестает быть проблемой каждого государства в отдельности. Это общая угроза, преодолеть которую можно только совместными усилиями. Для достижения указанной цели необходимо выстраивать систему коллективной информационной безопасности с учетом современных угроз в киберпространстве. Что предполагает: во-первых, принятие соответствующих законов на национальном уровне; во-вторых, выработку единых международных стандартов, таких как унификация понятийного аппарата; в-третьих, определение

[98]Бедарев К.В. Противодействие преступлениям, совершаемым по мотивам расовой, национальной или религиозной ненависти или вражды в сети Интернет. Краснодар. 2015. С. 110.

круга деяний, подлежащих криминализации; в-четвертых, имплементацию международных норм в национальное уголовное законодательство.

Подводя итог вышеизложенному можно утверждать следующее: для эффективной борьбы с экстремизмом в социальных сетях необходимо наличие действенного механизма по осуществлению непрерывного мониторинга и оперативного блокирования противоправного контента. В рамках этого необходимо развивать взаимодействие правоохранительных органов с руководством социальных сетей для блокировки конкретного пользователя, распространяющего экстремистские материалы, блокировки экстремистских групп, в пределах социальной сети, что позволит избежать полного блокирования ресурса из-за наличия там указанных материалов. Так же необходимо отметить, что, не смотря на усилия правоохранительных органов по выявлению и блокировки экстремистского контента в социальных сетях, рост распространения экстремистских материалов сохраняется. Все это свидетельствует о несовершенстве государственного регулирования вопроса распространения экстремизма в социальных сетях в связи с чем перспективным направлением становится создание правовых режимов распространения информации через информационно-коммуникационные сети в части регламентации интернет-отношений по распространению информации при обеспечении баланса интересов всех участников такой коммуникации и их гармонизации с основами публичного правопорядка. Таким образом, для разрешения проблемы распространения экстремизма в социальных сетях в настоящее время необходимо использовать весь арсенал имеющихся мер от внесения изменений и дополнений в законодательство, взаимодействия с гражданским обществом, усовершенствования работы правоохранительных органов до налаживания стабильного международного сотрудничества в данной сфере и использование иных мер.

Заключение. Экстремизм в социальных сетях за сравнительно небольшой период времени превратился в одну из острейших проблем нашей страны.

Несмотря на принимаемые меры по профилактики, криминальная обстановка в данном сегменте остается весьма сложной, о чем свидетельствует ежегодный рост преступности экстремистского характера в целом, и экстремизма в социальных сетях в частности. По данным официальной статистики количество зарегистрированных преступлений экстремисткой направленности, совершаемых в социальных сетях, в период с 2013 по 2015 гг в целом по России увеличилось на 34,2%. Проявление экстремизма в социальных сетях по формам и способам отличается значительной разнообразностью, что, при отсутствии единого общепризнанного подхода к толкованию понятия «экстремистская деятельность» и квалифицирующих признаков, значительно усложняет работу правоприменителя по профилактике экстремизма в социальных сетях и уголовно-правовой защите общества от крайне радикальных деяний. Практика уголовных и административных дел показывает, что большинство преступлений и правонарушений экстремистской направленности совершенно в «ВКонтакте» - социальной сети потенциальную аудиторию которой составляет молодежь (64,33% участников). При этом экстремисты используют сеть «Интернет»

не только для поиска и вербовки сторонников, массового распространения заведомо экстремистских материалов, публичных призывов к осуществлению экстремистской деятельности, но и для создания сетей, координации и планирования своей противоправной деятельности, осуществления контроля за фактическим проведением мероприятий, а также поиска спонсоров, поддерживающих их радикальные идеи. Учитывая цели экстремистской деятельности, а так же масштабы ее распространения в социальных сетях очевидна необходимость детального изучения комплекса причин и условий, обуславливающих рост «киберэкстремизма» в России.

Проведенный анализ публикаций и научных исследований по данному вопросу показал, что детерминанты экстремизма в социальных сетях весьма многообразны и охватывают все важнейшие сферы жизнедеятельности современного общества. В качестве общих причин и условий можно выделить: спад экономики; снижение производства; постоянно растущая безработица; снижение уровня жизни и обнищание населения; усиление имущественного неравенства и расслоения; замедление темпов формирования среднего слоя; расширение криминальных кругов за счет числа маргинализированных и люмпенизированных людей; неконтролируемый процесс миграции и отсутствие четкой миграционной политики; кризис современного общества; проблемы института семьи и брака; экстремальное сознание, переходный, не устоявшийся, во многом маргинальный социальный статус, а так же не сформированность политического, экономического, религиозного сознания основных субъектов рассматриваемой категории преступлений - молодых людей; нарастающее вмешательство западной инородной культуры в традиционное российское пространство, в результате которого происходит деформация мировоззрения у части молодежи; отсутствие позитивных образов самореализации; негативное воздействие средств массовой информации; деструктивные социально-культурные явления; отсутствие эффективной государственной молодежной политики. К частным детерминантам «киберэкстремизма» исследователи относят: открытый доступ к социальным сетям; экстерриториальность и анонимность общения в сети «Интернет»; возможность регистрировать доменные имена сайта на одной территории, а размещать информацию на другой, используя при этом различные технические средства; латентность преступлений изучаемой направленности; относительную редкость и «точечный характер» их проявлений; особую сложность в расследовании дел, в частности, при правовой квалификации, доказывании, установлении личности лица, совершившего инкриминируемое преступление (идентификация «виртуальной личности» с реальным субъектом конкретного правоотношения), его вины, а так же признании, размещенных этим лицом материалов экстремистскими, несовершенство антиэкстремистского законодательства. При этом следует отметить, что борьба с преступностью экстремистского характера в социальных сетях будет эффективной при условии решения как можно большего числа перечисленных детерминантов.

На сегодняшний день выделяют общую и специальную профилактику экстремизма в социальных сетях. Субъектами первой являются:федеральные органы

государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, антитеррористические комиссии, правозащитные организации, образовательные учреждения. Участниками второй - правоохранительные органы в целом (ГУУР МВД России, ГУЭБ и ПК МВД России, ГУОООП МВД России, прокуратура и т.д.), и специализированные службыв частности (ГУПЭ МВД России, Управление «К», ЦПЭ ГУ МВД России).

Приоритетными направлениями деятельности указанных выше субъектов является не только выявление и пресечение экстремисткой деятельности, но и применение воспитательных, пропагандистских, мер, направленных на предупреждение «киберэкстремизма». Блокировка и удаление негативного контента в социальных сетях как модераторами, администраторами, так и пользователями страниц в сети «Интернет», самостоятельно или же по указанию уполномоченного органа (Роскомнадзора), а так же внесение экстремистской информации в Федеральный список экстремистских материалов на сегодняшний день являются наиболее распространенными способами в борьбе с изучаемым негативным явлением. Несмотря на комплекс проводимых мероприятий, рост преступности сохраняется в связи с чем исследователи предлагают: ужесточить ответственность за распространение экстремистской информации через сайты социальных сетей в «Интернете»; внести в законодательство изменения, согласно которым провайдеры интернет-связи и сотовые операторы привлекались бы к субсидиарной ответственности за правонарушения, совершенные их клиентами в виртуальном пространстве; принять федеральный закон «Об электронном документе», положения которого регулировали бы информационные отношения в виртуальном пространстве; ввести обязательную контентную фильтрацию сайтов сети «Интернет» в учреждениях системы образования; улучшить координацию правоохранительных органов и субъектов гражданского общества в области контроля виртуального пространства; усовершенствовать программы и механизмы подготовки специалистов в области информационной безопасности. Кроме перечисленного необходимым условием эффективной борьбы с экстремизмом является наличие структур, успешно осуществляющих мониторинг социальных сетей и своевременно информирующих правоохранительные органы о фактах пропаганды экстремизма. Немаловажным представляется и развитие международного сотрудничества в сфере профилактики экстремизма в сети «Интернет».

Обобщая вышесказанное, следует отметить, что экстремизм в социальных сетях представляет реальную угрозу национальной безопасности и требует эффективного механизма государственного регулирования.

СИСТЕМА МЕР И МЕТОДИКА ОРГАНИЗАЦИИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ, ОБРАЗОВАТЕЛЬНОЙ, ПРОФИЛАКТИЧЕСКОЙ РАБОТЫ НА ЮРИДИЧЕСКОМ ФАКУЛЬТЕТЕ ФГБОУ ВО «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» *(В.А. Мазуров)*

Систему мер и методику организации научно-исследовательской, образовательной и профилактической работы юридического факультета по проблемам противодействия экстремизму в молодежной среде составляют следующие направления и методы:

1. Приказом ректора университета в 2011 году *образован Научно-образовательный центр «Правовое обеспечение противодействия экстремизму и терроризму» (далее Центр).*

Основными целями Центра являются:

- Организация и координация работы подразделений университета в научно-исследовательской, образовательной, профилактической и экспертно-консультационной сфере по правовому обеспечению противодействия экстремизму и терроризму.

- Установление и развитие сотрудничества с органами законодательной, исполнительной, судебной власти, правоохранительными органами, учебными заведениями Алтайского края по участию в мероприятиях, направленных на повышение уровня толерантности в регионе.

Основными задачами Центра являются:

- Организация и проведение *научных исследований экстремизма и терроризма* в современной России, Сибирском регионе и Алтайском крае.

- Организация и проведение *конференций, семинаров, заседаний круглого стола и иных научно-практических мероприятий в университете,* а также предусмотренных в планах, программах Главного управления образования и молодежной политики Алтайского края, Комиссией Алтайского края по противодействию экстремизму, Комиссией Алтайского края по противодействию терроризму.

- Формирование *научной, учебно-методической базы для использования в образовательном процессе* и профилактике экстремизма и терроризма в молодежной среде.

- Установление международного *сотрудничества в научно-исследовательской и образовательной сферах* по правовому обеспечению противодействия экстремизму и терроризму.

2. *Методы по организации и проведению научно-исследовательской и образовательной работы:*

- Монографии, статьи в научные журналы и их использование в учебном процессе. (Монографии, опубликованные в соавторстве с учеными правоведами вузов

Республики Казахстан, с ответственными сотрудниками Администрации Алтайского края, статьи в научных журналах Республики Казахстан, России).

- Научно-практические *конференции, семинары, круглые столы, конкурсы на лучшую научную работу, лучший учебный видеофильм. Сборники научных работ преподавателей и студентов университета, юридического факультета и учебные видеофильмы – в учебном процессе*. («Глас народов», «Мы», «Экстремизм – путь в никуда», «Обыкновенный вахобизм», «ИГИЛ», «Замужем за ИГИЛ» и т.д.).

- *Презентации на лекциях* и практических занятиях по рассматриваемой тематике.

(«Россия – это мы», «Толерантность», «Философско-правовые подходы к определению экстремизма», «Психологические критерии и оценка Экстремистских проявлений в юношеском возрасте» и т.д.).

- *Открытые лекции* по вопросам профилактики экстремизма в молодежной среде с участием ответственных сотрудников Комиссии Алтайского края по противодействию экстремизму, Центра противодействия экстремизму ГУ МВД РФ по Алтайскому краю.

- *Вовлечение студентов в научно-исследовательскую деятельность* по изучению причин и условий распространения среди молодежи экстремистских настроений, проявлений и эффективности государственных и общественных мер профилактического характера, а также разработке предложений по совершенствованию законотворческой и правоприменительной практике противодействия экстремизму. Использование эмпирического материала в учебном процессе. Выступление авторов научных разработок перед сокурсниками, а также в мероприятиях по правовому просвещению населения и в первую очередь молодежи (например, проект края «Юристы – населению» в 2014г.).

- *Информация о результатах научных исследований, Сборники научных статей преподавателей и студентов, иные источники размещены на Едином образовательном портале университета Moodle, на сайте юридического факультета, на странице НИРС по уголовному, уголовно-исполнительному праву, криминологии для использования в учебном процессе.*

- Научно-исследовательская и профилактическая работа *проводится под патронажем Департамента Администрации Алтайского края по обеспечению региональной безопасности, Главного управления образования и молодежной политики Алтайского края, во взаимодействии с ЦПЭ ГУ МВД РФ по Алтайскому краю, БЮИ МВД РФ,* вузами Республики Казахстан, Армении и др.

(Научно-практические конференции, образовательные семинары для студентов вузов края, круглые столы с участием студентов, открытые лекции).

- В настоящее время проводится международный конкурс на лучшую научную работу студентов на тему» Актуальные проблемы противодействия экстремизму и терроризму в современном мире и пути их решения». Студенты юридического факультета выезжают на стажировку в вузы Республики Казахстан, где выступают с докладами по вопросам профилактики экстремизма в молодежной среде.

На кафедре уголовного права и криминологии, на протяжении ряда лет работают *студенческие кружки* по углубленному изучению уголовного права России и криминологии. Одним *из приоритетных направлений* работы кружков является *подготовка студентов к участию в научно-практических конференциях, семинарах, конкурсах научных работ и иных научных мероприятиях*.

В рамках программы работы *Регионального научно-методического центра правовой и технической защиты информации* проводится ежегодная *всероссийская студенческая научно-практичебская конференция,* на которой студенты юридического и физико-технического факультетов обсуждают актуальные проблемы защиты охраняемой законом информации. По результатам конференций публикуются Сборники.

Таким образом, можно говорить о том, что имеет место сложившаяся система мер по организации научно-исследовательской работы студентов. В *целях активизации научно-исследовательской работы студентов* факультета, углубления их теоретических и практических знаний, считаем целесообразным создать дополнительные условия для реализации творческого потенциала обучающихся. В этой связи, предлагается *учредить на факультете электронный сборник научных работ преподавателей и студентов, который размещать на сайте юридического факультета.*

ВСЕМИРНАЯ СЕТЬ «ИНТЕРНЕТ» КАК СРЕДСТВО ПРОФИЛАКТИКИ ИДЕОЛОГИИ ТЕРРОРИЗМА В СОВРЕМЕННОМ МИРЕ *(Косенко Д.В., Шалабод К.В.)*

Введение. Современный период развития российского общества, связанный с построением демократического правового государства, предполагает повышение эффективности деятельности правоохранительных органов, необходимость поиска новых, нетрадиционных форм борьбы с криминальными угрозами, в числе которых особое место занимают преступления террористической направленности. Последние, в своих самых различных формах и проявлениях, становятся для многонациональной и полирелигиозной России одним из опаснейших факторов, угрожающих целостности страны и единству нации.

Явление терроризма весьма динамично развивается и с каждым днем приобретает все новые черты и характеристики. Так террористические организации все активнее используют достижения компьютерных технологий, внедряя в свою деятельность, прежде всего, те из них, которые достаточно эффективно воздействуют на массовое общественное сознание.

Однако у данного явления есть и другая сторона: правоохранительные органы и общественные организации используют всемирную сеть «Интернет» для профилактики преступлений террористической направленности. Потенциал и коммуникативные возможности сети «Интернет», социальных, локальных и файлообменных компьютерных сетей используются в качестве своеобразной информационной площадки дачи рекомендаций гражданам по действиям при угрозе совершения террористического акта, для интерактивного обучения вопросам тактики действий, организации правового воспитания.

Объектом исследования является комплекс общественных отношений, связанных с использованием сети «Интернет» как средства профилактики идеологии терроризма в современном мире.

Предметом исследования являются научная литература, интернет-порталы и сайты, занимающиеся борьбой с идеологией терроризма.

Цель данной работы – комплексный анализ влияния всемирной сети «Интернет» на профилактику идеологии терроризма в современном мире.

Для достижения заявленной цели в работе решаются следующие задачи:

– изучить понятие и признаки терроризма, отличие от террора;

– оценить роль всемирной сети Интернет в профилактике идеологии терроризма;

– дать характеристику сайтам, занимающимся профилактикой идеологии терроризма.

Методологическую основу исследования составляют общенаучные (в частности, анализ, индукция, дедукция, исторический метод и пр.) и специально-криминологические методы познания.

Общая характеристика терроризма. Нашествие терроризма, ставящее под угрозу нормальное существование мироустройства, требует от мирового сообщества поиска эффективных методов противодействия. За последние 30 лет проведены десятки конференций международного уровня, посвященные поиску путей борьбы с этим злом. В них принимали участие руководители государств, представители спецслужб и правоохранительных органов, общественных организаций и средств массовой информации. Однако до сих пор не выработано единого определения понятию «терроризм». Например, Организация Объединенных Наций ведет интенсивную работу в данном направлении с момента учреждения в 1972 г. в своем составе Комитета по международному терроризму, но так и не может прийти к единому знаменателю.

Термин «террор» по некоторым исследованиям, как отмечает А. Ю. Яковлев, возник «в период правления римского диктатора Суллы, практиковавшего казнь людей по любому ничтожному поводу. Другие приписывают авторство французскому мыслителю Ш. Монтескье, переведшему слово с латинского на французский для описания атмосферы страха деспотического государства»[99].

Таким образом, отдельные ученые считают, что термин «террор» перевел французский просветитель, мыслитель Ш. Л. Монтескье с латинского на французский язык для характеристики деспотического государства. Это связано с тем, что, по мнению Ш. Л. Монтескье: принцип деспотического правления – страх, выражающийся в нагнетании атмосферы страха и террора правителем на подданных[100].

Другие авторы, в частности А. Р. Бахтеева, придерживаются мнения, что «понятие террор ввел Аристотель для обозначения особого типа ужаса, который овладевал зрителями трагедии в греческом театре. Это был ужас перед небытием, представленным в форме боли, хаоса, разрушения. Считается, что осмысление террора посредством театра породило ритуал суда как разновидности театра, побеждающего террор через закон. Но в политический лексикон Европы слово «террор» вошло в XIV в., когда с латыни на французский были переведены сочинения древнеримского историка Тита Ливия»[101].

Как видим, среди исследователей, изучающих истоки происхождения термина «террор», нет единого мнения.

По мнению В. Шестакова «Террор в буквальном переводе с латыни означает «ужас». Наведение на людей ужаса было одним из инструментов политики на протяжении многих веков. Слово «террор» впервые появилось в политическом контексте во времена якобинской революции и массовых казней. В Новое время терроризм начали использовать также «независимые организации» и частные лица. Стали происходить покушения на монархов, президентов, банкиров и других

[99] Яковлев А. Ю. И вновь о терроризме: еще одна попытка найти его дефиницию // Социально-гуманитарные знания. 2012. № 4. С. 118 – 119.
[100] История политических и правовых учений / под общ. ред. О. В. Мартышина. М., 2007. С. 194.
[101] Бахтеева А. Р. Политический терроризм как социальное явление современности: дис. канд. социолог. наук. М., 2010. С. 16.

влиятельных особ. Постепенно власть террора нарастала. Но в тех условиях террор не мог носить массового характера. Лишь в конце XX в. стало ясно, что терроризм – это глобальная угроза нашей цивилизации»[102].

Таким образом, наиболее распространенное значение термин «террор» получил в период якобинской революции, проходившей в конце XVIII в. во Франции, ознаменовавшись массовыми казнями. Но и до этого периода нагнетание ужаса на людей применялось несколько веков в качестве одного из инструментов политической деятельности.

К сожалению, деятельность по противодействию терроризму осложнена таким фактором, как наличие огромного числа взаимоисключающих определений, возникших в результате различного подхода к этому явлению. В частности, в умах людей часто ставится знак равенства между террором и терроризмом, которые нередко трактуются достаточно свободно, что, конечно же, неприемлемо для единообразного понимания проблемы. В отличие от терроризма, характеризующегося крайними взглядами части общества и способностью этой части на мотивированное политическое насилие над государством и обществом для достижения своих целей, террор является антонимом слову терроризм, т.к. подразумевает (в отличие от исторической ретроспективы, где эти понятия были если не идентичны, то весьма близки) деятельность государства, направленную на достижение целей путем мотивированного политического насилия над обществом.

Другой точкой зрения на понятия «террор» и «терроризм» является позиция Т.В. Герасименко, по мнению которой терроризм отличается от террора тем, что «…терроризм – это одноразово совершаемый акт либо серия подобных актов, имеющих не тотальный, массовый, а, напротив, локальный характер; …если террор – социально-политический фактор действительности, то терроризм – явление уголовно-правового свойства, и его насилие с целью понуждения к каким-либо действиям на фоне созданного состояния страха имеет не всеобщее, а местное значение»[103].

Главным, по мнению Т.В. Герасименко, между терроризмом и террором выступает разница в глобальности действий и количестве населения, подвергшегося насилию (терроризм – одна или несколько акций локального характера, а террор – деятельность массового характера), а также в том, что террор – это социально-политический фактор, а терроризм – уголовно-правовой.

Вместе с тем, подобную трактовку некоторые считают попыткой упростить понятия. Если брать террор за единое целое, а терроризм механически расчленить на отдельные акции (террористические акты), из совокупности которых он попросту состоит, которыми подпитывается и которые являются физическим проявлением терроризма, воплощением его способа достижения цели, то можно говорить о глобальности террора и малой значимости террористического акта, в противном случае следует согласиться, что терроризм и даже отдельный террористический акт

[102] Шестаков В. Террор – мировая война. М., 2003. С. 3.
[103] Герасименко Т.В. Понятие и признаки терроризма. [Электронный ресурс]. Правовая поисковая система «Консультант плюс».

могут быть не менее значимыми и кровавыми, чем акты террора.

Что такое «терроризм»? Многие источники говорят о понятии «терроризировать». Например, в Советском энциклопедическом словаре читаем: «Терроризировать (фр. terroriser, от лат. terror – страх, ужас) – преследовать, угрожая расправой, убийствами, держать в состоянии страха»[104]; в словаре С.И. Ожегова: «террор – это физическое насилие, вплоть до физического уничтожения, по отношению к политическим противникам»[105]. Из этого можно сделать вывод, что для многих исследователей террор и терроризм – идентичные понятия и напрямую связаны с насилием над политическими противниками с целью их устрашения или уничтожения.

Вместе с тем исследователь терроризма Е.П. Кожушко в своей монографии: «Современный терроризм: анализ основных направлений» противопоставляет понятия «терроризм» и «террор». В частности, автор говорит, что: «террор – это политика репрессий со стороны государства, опирающегося на мощь своих силовых институтов», а «терроризм – это насилие, осуществляемое со стороны политических группировок. Оружие террора – репрессии, оружие терроризма – террористический акт»[106]. При этом он, говоря о терроризме, не ведет речь только об уголовном насилии или насилии в отношении только политических противников, он говорит о насилии со стороны политически ангажированных групп, а это большая разница.

В настоящее время в мире существует несколько школ, которые трактуют понятие «терроризм», исходя их тех или иных научных подходов. В результате чего разработано несколько определений. Достаточно подробный анализ этих определений в своем диссертационном исследовании терроризма делает, например, А.К. Боташева. В частности, она выделяет несколько основных подходов (нормативистский, правовой, аналитический и синтетический), с приведением мнения ученых, являющихся их сторонниками[107].

Сторонник нормативистского подхода профессор истории Джорджтаунского университета У. Лакер считает терроризмом «незаконное использование силы против невиновных людей для достижения политических целей», при этом, добавив, что попытки выйти за рамки простого определения бесполезны, т.к. сам термин противоречив.

Второй подход к исследованию данной проблемы заключается в акцентировании на правовых аспектах определения. Этот подход присущ ряду государств Европы. Например, в Германии под терроризмом понимается использование преступных актов для достижения политических целей или способ, который позволяет создать политический беспорядок. Б. Гросскап, являющийся сторонником данного подхода, говорит о том, что терроризм определяется в Германии как нарушение закона и

[104] Советский энциклопедический словарь / Науч.-ред. совет: А.Н. Прохоров (председатель). М.: Советская Энциклопедия, 1981. С. 1335.
[105] Ожегов С.И. Словарь русского языка. М., 1978. С. 731.
[106] Кожушко Е.П. Современный терроризм: анализ основных направлений. Минск: Харвест, 2000. С. 10.
[107] Боташева А.К. Политический терроризм: детерминация и формы проявления.: Дис. … канд. полит. наук. Ставрополь, 2004. С. 20.

против террористов, которые преступают закон, могут быть приняты определенные правовые меры.

Сторонники третьего подхода к решению проблемы определения терроризма – «аналитического», критикуют нормативный подход за «моралистичные» и «эмоциональные» определения, а правовой – за узкую правовую направленность, которая не исчерпывает все связанные с терроризмом аспекты. «Аналитики» утверждают, что правовой подход выпячивает правовую сторону, игнорируя необходимость всестороннего анализа терроризма, с точки зрения социального феномена, с выделением и оценкой симптомов, способствующих этому явлению. Например, М. Креншоу считает, что сам террористический акт, цели и возможность политического успеха являются факторами, которые должны быть проанализированы перед использованием термина «терроризм».

Четвертым направлением является так называемый «синтетический» подход. Представитель данного подхода А. Шмидт, проанализировав десятки определений понятия «терроризм», дал на их основе свое, состоящее из 13 элементов, наиболее часто встречавшихся в исследованных им определениях. В результате им было дано определение следующего содержания: «Терроризм – это насильственный метод или угроза его использования, применяемые неправительственными законспирированными индивидами, группами или организациями в мирное время, осуществляемые с помощью дискретных действий, направленных на различные объекты с определенными целями или эффектом»[108]. Как видим, подходы весьма разнообразны и единства между ними нет.

Несмотря на все разнообразие в подходах к определению понятия «терроризм», юридически значимыми для нас являются понятия, данные в Федеральном законе № 35-ФЗ «О противодействии терроризму» от 6 марта 2006 г. и Уголовном кодексе Российской Федерации. В ст. 3 Федерального закона «О противодействии терроризму» терроризм определяется как «идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий»[109]. Данное определение в целом подчеркивает цель терроризма и субъекты, на которые направлено воздействие (оказание давления на органы государственной власти, органы местного самоуправления или международные организации с побуждением принятия определенного решения); способом достижения цели выступает устрашение населения или иные формы противоправных насильственных действий.

Об этом же в своем исследовании говорят П.А. Агапов и К.В. Михайлов, утверждая, что «современное понятие терроризма основными признаками закрепляет, во-первых, цель – воздействие на принятие решения органами государственной власти,… и, во-вторых, способы достижения этой цели – устрашение населения и

[108] Боташева А.К. Политический терроризм: детерминация и формы проявления.: Дис. … канд. полит. наук. Ставрополь, 2004. С. 22.
[109] О противодействии терроризму: федеральный закон от 06.03. 2006г. №35-ФЗ (ред. от 06.07.2016г.) // Российская газета.- 2006г.- №48.

(или) иные формы противоправных насильственных действий»[110]. Исходя из общеправового определения, даваемого такому глобальному явлению, как «терроризм», законодателем делается следующий шаг, направленный на конкретизацию проявления терроризма посредством вычленения в нем отдельных элементов – актов терроризма или «террористических актов». При этом понятие «террористический акт», описываемое в п. 3 ст. 3 настоящего Федерального закона, привело к изменению законодательства и переносу данного понятия в Уголовный кодекс РФ. Следствием этого стало появление нового уголовно-правового понятия «террористический акт», принятого в ст. 205 УК РФ, которое определяется как совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в тех же целях.

Таким образом, в российском законодательстве закреплено как общеправовое понятие «терроризм», так и уголовно-правовая составляющая этого явления («террористический акт»). Нечто подобное предлагал провести Л.Д. Гаухман. Правда, он говорит только о том, что наиболее приемлемым было бы, если «…законодатель определил понятия терроризма в общеправовом и уголовно-правовом значениях разными терминами»[111].

Однако несмотря на всю сложность и неоднозначность такого явления, как «терроризм», если мы говорим о его угрозе личности, государственным устоям и миру и человечеству в целом, а также необходимости борьбы с ним, то и рассматривать его необходимо комплексно, а не давая в зависимости от ситуации то одно, то другое определение. Более того, терроризм нужно рассматривать как своего рода «сверхпреступление». Именно об этом говорит, например, А.Г. Хлебушкин[112].

Вместе с тем, главной целью терроризма и лиц, осуществляющих террористическую деятельность, является не просто оказание давления на власти путем осуществления актов устрашения с целью принятия определенного решения, а именно безоговорочное подчинение. Таким образом, объектами терроризма при осуществлении террористических актов выступают важнейшие сегменты в жизни общества – его безопасность, а также безопасность государств, в лице их представителей и всего международного сообщества.

Признаки терроризма. Говоря о терроризме, необходимо уяснить, что, во-первых, терроризму присущи не широкомасштабная компания по ведению боевых действий, а отдельные акции, направленные не только и не столько против

[110] Агапов П.А., Михайлов К.В. Уголовная ответственность за содействие террористической деятельности: тенденции современной уголовной политики. Саратов, 2007. С.19-20.
[111] Гаухман Л.Д. Уголовно-правовая борьба с терроризмом. [Электронный ресурс]. Правовая поисковая система «Консультант плюс».
[112] Хлебушкин А.Г. Экстремизм: уголовно-правовой и уголовно-политический анализ / Отв. ред. Н.А. Лопашенко. Саратов, 2007. С. 44-45.

вооруженных сил противника и его правоохранительных органов и спецслужб, а в основном против мирного населения, выступающего в этом случае главной мишенью для ударов, с целью оказать давление на политическую власть. Террористы могут требовать принятия от государства решения, вплоть до его полного самоуничтожения. При этом для террористов важнейшее значение имеет не способ ведения войны, не захватываемая территория и экономические ресурсы, а тот шок и страх, который вызовет та или иная их акция. Данная цель подразумевает под собой как можно более кровавые и бесчеловечные действия по отношению к лицам, подвергшимся атаке. «Войны, в том числе и гражданские, – писал У. Лакер, – во многом носят достаточно предсказуемый характер, они происходят, что называется, средь бела дня, противоборствующие стороны и не думают окутывать себя и свои действия ореолом тайны. Даже гражданская война соблюдает те или иные правила, в то время как главные признаки терроризма – анонимность и отрицание каких бы то ни было норм»[113].

Во-вторых, терроризму необходимы конспирация и анонимность. Любая огласка может затруднить исполнение террористического акта. Вместе с тем некоторые исследователи пытаются оспорить данный признак, заявляя о том, что ряд террористических организаций (ЭТА, ИРА и т.д.) уведомляют о готовящемся теракте. На это можно возразить только то, что данная мысль ошибочна изначально, так как речь ведется о спланированной и подготовленной в тайне акции, в противном случае акция просто не смогла бы состояться. Предоставление же информации об этой акции – своеобразная пиар-компания, которая не имеет ничего общего с заботой о жизни людей, как это может показаться на первый взгляд, а преследует все ту же цель – создание атмосферы страха и неуверенности у населения, а заодно и пропаганда своего мнимого миролюбия.

В-третьих, терроризму необходимо информирование населения о террористических актах и их результатах. Один из наиболее значимых способов, дающий возможность достижения главной цели – запугать население и через него заставить государство выполнить требования террористов. Для этого терроризму необходимы средства массовой информации, которые как раз и ориентируются на сенсации и трагедии, которые терроризм и способен им дать. Современный террористический акт по своей сути является детищем средств массовой информации, был ими взращен, вскормлен и доведен до абсурдного, но зрелищного и трагического шоу с кровопролитием. Огромные возможности активного воздействия СМИ на сознание и поведение населения как раз и свидетельствует об огромном возрастании их роли в современном обществе.

В четвертых, терроризму присуща примитивная идеология. В основном идеология терроризма выражена сравнительно узко по содержанию и реализуется средствами общественной психологии, религиозными постулатами и догмами. Для террористов вооруженная борьба становится важнее процесса идеологического обоснования. Хотя необходимо отметить, что сейчас прослеживается тенденция

[113] Кожушко Е.П. Современный терроризм: анализ основных направлений. Минск: Харвест, 2000. С. 366.

терроризма все больше использовать идеологическое обоснование своей деятельности, используя для этого, в первую очередь, СМИ и Интернет.

Таким образом, видится, что давая определение понятию «терроризм», необходимо выделять такие важнейшие признаки, присущие этому явлению, как: общественная опасность деяния, его нелегитимность в глазах общества, анонимность действий при подготовке акций и широкая огласка их совершения и их результатов, наличия, присущего акциям терроризма, характера принуждения власти к действиям или бездействию и устрашения населения.

Интернет как средство профилактики идеологии терроризма. Роль всемирной сети Интернет в профилактике идеологии терроризма. *В* настоящее время для большинства населения использование сети «Интернет» стало неотъемлемой частью их повседневной жизни. Поиск информации, просмотр фильмов, дистанционная работа – основные сферы использования Интернета рядовым пользователем. Однако не все используют его для таких целей. Многие международные террористические группировки используют данный информационный ресурс как средство пропаганды своих идей. В настоящее время насчитывается около 10 тысяч сайтов, посвященных террористическим акциям. К сожалению, данное число не предел, с каждым годом оно значительно увеличивается.[114]

Е.П. Ильин, первый заместитель руководителя аппарата Национального антитеррористического комитета, в своем докладе на III Всероссийской научно-практической конференции «Концепции противодействия терроризму в Российской Федерации» отметил, что в современный период наибольшие угрозы распространения идеологии терроризма связаны с использованием террористическими и экстремистскими организациями сети Интернет и мобильной связи для организации скрытых каналов и пропаганды преступной деятельности.[115]

В литературе[116] выделяют следующие группы причин, обуславливающих использование сети Интернет в террористических целях:

1. Политические причины, которые как внешние факторы (процессы глобализации и процессы столкновения политических интересов разных государств), так и внутренние факторы (политическая нестабильность и конфликты внутри государства).

2. Социальные причины, к которым относят разрушение культурного пространства, малоэффективную систему образования и здравоохранения, проблемы демографии.

---

[114] Воронцов, С.А. О необходимости совершенствования подходов к обеспечению национальной безопасности России в информационной сфере / С.А. Воронцов, А.Г. Штейнбух // Наука и образование: хозяйство и экономика; предпринимательство; право и управление.- 2015.- №9 (64).- С. 100-108.

[115] Ильин, Е.П. Доклад первого заместителя руководителя аппарата НАК / Е.П. Ильин // Материалы III Всероссийской научно-практической конференции «Концепции противодействия терроризму в Российской Федерации».- Том. 1.- М., 2012.- С. 3-16.

[116] Воронцов, С.А. Формирование угроз безопасности Российской Федерации как следствие кризиса культуры / С.А. Воронцов // Гуманитарные и социально-экономические науки.- 2013.- №5.- С. 111-115.

3. Экономические причины, среди которых выделяют безработицу, инфляцию, растущую социальную дифференциацию общества.

Также технические характеристики, которым обладает сеть Интернет, в наибольшей степени благоприятствуют распространению информации террористического характера. Так, например, этому способствует:

1. Широкий охват аудитории;
2. Доступ к данной сети в любой точке мира, независимо от географического положения;
3. Высокая скорость и лавинообразный характер распространения информации;
4. Возможность анонимного размещения материалов;
5. Использование лазеек в несогласованности в законодательствах стран мира в области «компьютерного права» (например, сайт чеченских сепаратистов «Кавказ-Центр», который в некоторое время успешно работал на шведских, а ныне на американских серверах).

В большинстве случае пропаганде ориентирована, прежде всего, на молодежь, что связано не только с тем, что молодое поколение активно используют информационные ресурсы, но и с тем, что молодежь является наиболее восприимчивой и легко может поддаться течению той или иной идеологии. Также в сами экстремистские группировки входят чаще всего молодые специалисты, которые владеют различными навыками, хакерскими способностями. Так, например, террористы могут найти своих сторонников через опросы различного характера, по которым они смогут определить отношение человека к той или иной проблеме. Затем они связываются с такими пользователями и налаживают с ними контакт, рассказывая о своей деятельности и привлекая их на свою сторону. Далее из всей аудитории завербованных выделяются небольшие автономные группы, которые действуют уже объединившись, выполняют различные задания, согласно инструкциям своих «наставников».[117]

Террористические организации используют «всемирную паутину» не только в целях агитации и пропаганды, а также для решения широкого круга задач, включая финансирование, подготовку исполнителей, подстрекательство к совершению актов терроризма, а также сбор и распространение информации в террористических целях.

Но, помимо наличия данной информации в сети, существуют также эффективные средства противодействия им. С идеологией терроризма можно бороться лишь идеологическими методами, а значит одним из направлений профилактики борьбы с террористической деятельностью в сети Интернет, следует обозначить – воспитание молодежи, формирование ее гражданской идентичности. В настоящее время в Российской Федерации открыто множество сайтов, занимающихся борьбой с идеологией терроризма и экстремизма. Характеристика основным сайтам,

[117] Сивопляс, К.О. О противодействии идеологии терроризма в сети «Интернет» / К.О. Сивопляс // Ростовский научный журнал.- 2016.- №7.- С. 5-12.

действующим в целях профилактики идеологии терроризма, будет дана в следующем параграфе.

Характеристика сайтов, действующих с целью профилактики идеологии терроризма. Информационное противодействие терроризму и экстремизму в сети Интернет можно разделить на два направления: ограничение доступа к запрещенным материалам и информационно-просветительская деятельность. Поскольку в первом направление, как правило, работают органы государственной власти и общественные объединения, деятельность которых сложно подробно рассмотреть и оценить, то в данной работе мы остановимся на общей характеристике сайтов, действующих в целях профилактики идеологии терроризма.

Одним из основных сайтов, действующих с целью формирования единого информационного антитеррористического пространства, является сайт Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет (НЦПТИ).[118]

НЦПТИ создан для решения задач, поставленных Министерством образования и науки Российской Федерации. Работа Центра направлена на активное противодействие распространению идеологии терроризма и экстремизма, совершенствование работы по информационно-пропагандистскому обеспечению антитеррористических мероприятий в сети Интернет, привлечению молодежи и студентов к разработке теоретических и методологических основ противодействия идеологии терроризма.

В перечень основных задач, которые решаются НЦПТИ, входят:

1. Мониторинг и анализ интернет-пространства с целью выявления фактов пропаганды идеологии терроризма и экстремизма;
2. Организация и проведение мероприятий, направленных на профилактику идеологии терроризма в молодежной среде и сети Интернет;
3. Информационно-аналитическое обеспечение органов государственной власти Российской Федерации по интересующим тематикам;
4. Анализ и прогнозирование развития ситуации в регионах страны и мира.

Для решения поставленных задач НЦПТИ создал несколько информационно-просветительских ресурсов.[119]

Во-первых, создан и поддерживается информационно-аналитический ресурс «НЦПТИ.РФ», на котором размещаются методические рекомендации, памятки, аналитические статьи, иллюстрации. Также на сайте функционирует «горячая линия», посредством которой любой пользователь сети Интернет может сообщить о противоправном контенте, с которым он столкнулся на просторах всемирной сети.

---

[118] Сайт Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет [Электронный ресурс]. – Электр. дан. – Заглавие с экрана. URL: http://нцпти.рф (дата обращения 15.11.2017).

[119] Чурилов, С.А. Экспертная интернет-платформа как средство коллегиальной разработки методов информационного противодействия терроризму и экстремизму / С.А. Чурилов // Материалы II Всероссийской научно-практической конференции «Роль средств массовой информации и Интернета в предупреждении терроризма».- Том. 1.- М., 2013.- С. 87-92.

Во-вторых, в социальной сети «ВКонтакте» создана группа «НЦПТИ», в которой для молодежной аудитории в доступном формате публикуются новостные материалы, видеоматериалы и справочные иллюстрации по теме профилактики идеологии терроризма.

В-третьих, НЦПТИ выпускает периодическое издание «Обзор.НЦПТИ», которое предназначено для обмена опытом между различными ведомствами и отдельными специалистами в области профилактики и противодействия радикальным идеология, информационного противоборства и защиты информации.

В-четвертых, создана площадка для обсуждения вопросов комплексной безопасности в образовательных и научных учреждениях Российской Федерации – это информационно-практический форум «Безопасность и образование». Форум объединяет представителей Министерства образования и науки Российской Федерации, Федеральной службы безопасности Российской Федерации, Министерства внутренних дел Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации, образовательных и научных организаций.

Следующий сайт, занимающийся пропагандой антитеррористической идеологии - «Наука и образование против террора»[120].

Данный сайт создан с целью продвижения доступной для понимания пользователей информации о позиции научного сообщества по проблематике антитеррористической деятельности, ее социально-экономических аспектах, эффективности действий всех ветвей российской власти на данном направлении. Участниками проекта являются преподаватели, сотрудники и студенты высших учебных заведений России, российские и зарубежные специалисты в области противодействия терроризму, которые ставят задачу объединить ученых, преподавателей и студентов российских вузов для научного противодействия насилию и террору. На портале размещается информация, способствующая неприятию пользователями идеологии терроризма и экстремизма, уважительному отношению к духовным ценностям религиозных конфессий различного рода. Согласно информации, представленной на сайте, портал посещают жители разных стран, таких как Казахстан, Таджикистан, Польша, Канада, Германия и др., что позволяет сделать вывод, что этот сайт вызывает интерес как у российских граждан, так и у зарубежных пользователей.

Также следует выделить сайт «Молодежь за Чистый Интернет».[121] Данный интернет-портал также, как и сайты, указанные выше, создан с целью привлечения политически активной части населения для поиска решений проблем терроризма и экстремизма в современном мире, идеологической борьбы с ними. Данный сайт также распространен не только в России, но и в других странах.

---

[120] Сайт «Наука и образование против террора» [Электронный ресурс]. – Электр. дан. – Заглавие с экрана. URL: http://www.scienceport.ru (дата обращения 15.11.2017).

[121] Сайт «Молодежь за чистый интернет!» [Электронный ресурс]. – Электр. дан. – Заглавие с экрана. URL: http://www.truenet.info (дата обращения 15.11.2017).

Наряду с указанными сайтами, деятельность которых в большей степени несет просветительский и информативный характер, пользователи также имеют доступ к сайтам федеральных органов исполнительной власти, чья деятельность направлена на борьбу с терроризмом.

Указом Президента Российской Федерации от 15 февраля 2006 г. №116 «О мерах по противодействию терроризму»[122] в целях совершенствования государственного управления в области противодействия терроризму был образован Национальный антитеррористический комитет.

Так, согласно п. 1 данного Указа, Национальный антитеррористический комитет является коллегиальным органом, образованным в целях организации и координации деятельности по противодействию терроризму, осуществляемой федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации и органами местного самоуправления, а также антитеррористическими комиссиями и оперативными штабами в субъектах Российской Федерации, оперативными штабами в морских районах (бассейнах).

Основными задачами данного органа являются:

1. Мониторинг состояния общегосударственной системы противодействия терроризму, подготовка предложений Президенту Российской Федерации по формированию государственной политики и совершенствованию нормативно-правового регулирования в области противодействия терроризму;
2. Организация и координация деятельности по противодействию терроризму, осуществляемой федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, а также антитеррористическими комиссиями и оперативными штабами в субъектах Российской Федерации, оперативными штабами в морских районах (бассейнах);
3. Информационное сопровождение деятельности по противодействию терроризму.

На официальном сайте[123] комитета можно просмотреть всевозможные антитеррористические учения, контртеррористические операции, проведенные им, также на нем расположена информация о конференциях и круглых столах, находящаяся в открытом доступе, новостные сводки, а также информация о деятельности субъектов Российской Федерации в данном направлении. Так, одним из последних размещенных на сайте антитеррористических учений является командно-штабное учение «Арсенал - 2017», проходивший в Курской области в период с 1 по 2 ноября 2017 г. по теме «Организация и проведение мероприятий по пресечению террористического акта на объекте Вооруженных Сил Российской Федерации». Целью данного учения было отработка планирования мероприятий по противодействию терроризму, проверка сил территориальных подразделений

[122] О мерах по противодействию терроризму: Указ Президента РФ от 15.02.2006 №116 (ред. от 29.08.2017) // Собрание законодательства РФ.- 2006.- №8.- Ст. 897.

[123] Сайт Национального антитеррористического комитета [Электронный ресурс]. – Электр. дан. – Заглавие с экрана. URL: http://nac.gov.ru (дата обращения 15.11.2017).

федеральных органов исполнительной власти и органов местного самоуправления. Оперативными группами были проведены эвакуационные мероприятия, которые предусматривали сбор, транспортировку и размещение эвакуируемых граждан (население близлежащих населенных пунктов) в Клюквинскую СОШ, а также их медицинское и психологическое обслуживание.

Необходимо отметить также эффективность проведения антитеррористических идеологических работ с помощью Интернет-семинаров в режиме онлайн, которые могут посещать неограниченное количество заинтересованных пользователей.

Однако терроризм как явление постоянно развивается, подстраиваясь под изменения общественной жизни, поэтому деятельность по профилактике и борьбе с идеологией терроризма нуждается в постоянном реформировании и развитии. В литературе предлагается ввести следующие механизмы и инструменты для решения проблем противодействия идеологии терроризма: [124]

1. Развитие международного сотрудничества в области противодействия терроризму. Согласно п. 48 «Концепции противодействия терроризму в Российской Федерации»,[125] международное сотрудничество является необходимым условием обеспечения эффективности противодействия терроризму и осуществляется на основе и при строгом соблюдении принципов и норм международного права, а также в соответствии с международными договорами Российской Федерации. Это связано с тем, что, как правило, терроризм носит международный характер, не ограничиваясь границами одного государства, поэтому только общими усилиями можно влиять и в конечном итоге прекращать террористическую деятельность на ранних этапах её зарождения.

2. Создание большего количества Интернет-ресурсов с целью информационного противодействия экстремизму и терроризму в сети «Интернет».[126] Основными целями деятельности таких сайтов должны быть:

– Формирование единого информационного антитеррористического пространства в сети «Интернет» для освещения аналитической работы научного сообщества по выявлению и разъяснению сущности терроризма, его общественной опасности;

– Формирование стойкого неприятия обществом идеологии насилия;

– Привлечение граждан к участию в противодействии терроризму и экстремизму;

– Обсуждение проблем терроризма, экстремизма, национального и религиозного шовинизма и других негативных социально-политических и криминальных явлений в режиме онлайн.

---

[124] Бирюков, В.Г. Противодействие идеологии терроризма среди молодежи в сети Интернет / В.Г. Бирюков // Ростовский научный журнал.- 2016.- №5.- С. 28-36.

[125] Концепция противодействия терроризму в Российской Федерации: утверждена Президентом РФ от 05.10.2009 // Российская газета- 2009.- №198.

[126] Воронцов, С.А. О необходимости совершенствования подходов к обеспечению национальной безопасности России в информационной сфере / С.А. Воронцов, А.Г. Штейнбух // Наука и образование: хозяйство и экономика; предпринимательство; право и управление.- 2015.- №9 (64).- С. 100-108.

3. Проведение интернет-конференций с целью обсуждения актуальных проблем противодействия идеологии экстремизма и терроризма.

4. Проведение мероприятий по противодействию идеологии экстремизма и терроризма в школьных и высших учебных заведениях, что позволит сформировать в молодежной среде антиэкстремистские и антитеррористические настроения.

5. Развитие адаптивных навыков, необходимых молодежи для социализации и преодоления жизненных проблем: волонтерская работа; создание программ по формированию жизненных навыков и др.

6. Организация досуга молодежи посредством увеличения числа доступных секций и кружков, которые были бы действительно интересны современной молодежи.

Таким образом, можно сделать вывод, что роль сайтов, действующих в целях профилактики идеологии терроризма, в настоящее время достаточно велика, поскольку это обусловлено влиянием Интернета на жизнь человека. Однако нельзя забывать и о других средствах противодействия идеологии терроризма, потому что успех антитеррористической работы зависит от совокупного использования всех механизмов и инструментов для решения данной проблемы.

Заключение. В современном мире терроризм является одной из самых важных и опасных проблем, грозящих безопасности, как государств, так и отдельно живущих в них граждан. Отмечаемый в последние годы, как в Российской Федерации, так и за рубежом (Франция, Бельгия, Венгрия, Германия и др. страны) рост активности и масштабов деятельности террористических формирований, повышение уровня организованности проводимых ими многоступенчатых акций, четкое распределение ролей и обеспечение синхронности действий участников при строгом соблюдении ими конспирации и т.д. заставляют переосмыслить изменения в стратегии и тактике экстремистов XXI века и задуматься о соответствии современным реалиям существующей в Российской Федерации системы мер обеспечения безопасности личности, общества, государства, возможных направлениях повышения эффективности борьбы с экстремизмом и терроризмом.

Террористы, как известно, стремятся навязать свою идеологию обществу, в связи с чем, активно используют такие пропагандистские коммуникационные ресурсы как СМИ, Интернет. Поэтому органы государственной власти и местного самоуправления должны организовать адекватное противодействие идеологии терроризма.

В ближайшем будущем основными направлениями деятельности, которым следует уделить наибольшее внимание, должны стать следующие:

- привлечение общественности для выявления фактов пропаганды радикальных идей, сбора средств и другого;
- привлечение общественности к процессу удаления или частичного ограничения доступа к радикальным материалам в сети Интернет;
- анализ «обратной связи» – получение оценки профилактической литературы от целевой аудитории (студенты, школьники) для выработки дальнейших рекомендаций

по ее созданию и распространению (поскольку экспертное сообщество зачастую «варится» само в себе);

- формирование гражданского самосознания обучение медиабезопасности и противодействию интернет-манипуляциям;
- тиражирование технологий во всех федеральных округах Российской Федерации**.**

Необходимо помнить, что успех антитеррористической работы зависит от совокупного использования всех механизмов и инструментов для решения данной проблемы

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ *(Кузнецова Е.В., Яндиков М.С.)*

Введение. На современном этапе развития российского общества важное значение приобретают проблемы обеспечения его безопасности в целом, и информационной безопасности в частности. Активное и динамичное развитие информационных технологий, особенно компьютерной техники, в управленческой, производственной, коммерческой, банковской и иных сферах объективно требует повышения уровня обеспечения информационной безопасности. Актуальность темы исследования обусловлена тем, что в условиях всевозрастающей компьютерной грамотности набирает силу организованная преступность. Преступные группы и сообщества начинают активно использовать в своей деятельности новейшие достижения науки и техники. Для совершения преступлений преступниками все чаще применяются технические приемы и средства компьютерной техники и используются информационные линии связи, в том числе компьютерные сети. В связи с этим популярность приобретает термин «компьютерная преступность».

Целью исследования является изучение теоретических и практических аспектов, связанных с проблемами противодействия компьютерной преступности.

Для достижения заданной цели, необходимо решить ряд задач:

1. Изучить общую характеристику компьютерной преступности в современной России;

2. Рассмотреть основные детерминанты компьютерной преступности;

3. Раскрыть способы предупреждения компьютерных преступлений.

Объектом исследования являются общественные отношения, складывающиеся в сфере уголовно-правовой борьбы с компьютерной преступностью.

Предмет – понятие преступления в сфере компьютерной информации и проблемы, связанные с противодействием ей.

Методологическую и теоретическую основу проведенного исследования составляет общенаучный диалектический метод познания социально-правовых явлений, а также различные частно-научные методы: сравнительно-правовой, логико-юридический, системно-структурный, статистический, представляющие анализ соответствующей базы по рассматриваемой проблематике, обобщение и синтез точек зрения, представленных в источниках; и иные методы.

Степень разработанности темы. Общетеоретические подходы в изучении различных аспектов преступлений в сфере компьютерной информации отражены в научных трудах таких ученых, как Быков В.М., Евдокимов К.Н., Кесареева Т. П., Савиновский А.Н., Мазуров В.А., Поляков В.В., Трошин А.А. и других исследователей.

Нормативную основу исследования составили: Конституция РФ, уголовное

законодательство РФ, научные труды по уголовному праву.

В ходе исследования изучена статистическая информация, опубликованная на официальном сайте Министерства внутренних дел Российской Федерации.

Структура работы. Реферат состоит из введения, трех глав, заключения и списка использованных источников и литературы. Общий объем работы составляет 30 страниц.

Общая характеристика компьютерной преступности в современной России. Под компьютерными преступлениями понимаются противозаконные действия, в которых компьютер является либо объектом, либо орудием посягательства в сфере автоматизированной обработки информации.

Компьютерные преступления разделяются на:

1) Несанкционированный доступ и перехват. Содержит такие компьютерные преступления, как перехват информации, «компьютерный абордаж», кража времени - незаконный доступ в компьютерную систему, с намерением не оплатить услуги;

2) Изменение компьютерных данных с помощью таких угроз, как троянский конь, червь, логическая бомба, компьютерный вирус.

3) Компьютерные мошенничества. Бывают:

– связанные с хищением наличных денег из банкоматов;

– связанные с созданием поддельных устройств (карточек и пр.) – компьютерные подделки;

– связанные с манипуляцией с программами ввода-вывода (метод подмены данных кода);

– связанные с платежными средствами;

– телефонное мошенничество.

4) Незаконное копирование информации. Бывает следующих видов:

– незаконное копирование, распространение или опубликование программного обеспечения, защищенного законом;

– незаконное копирование топографии полупроводниковых изделий - копирование, без права на то, защищенной законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью, без права на то, топографии или самого полупроводникового изделия, произведенного с использованием данной топографии.

5) Компьютерный саботаж. Предполагает:

– саботаж с использованием аппаратного обеспечения - ввод, изменение, стирание, подавление компьютерных данных или программ; вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы;

– саботаж с программным обеспечением - стирание, повреждение, ухудшение или подавление компьютерных данных или программ без права на то.[127]

[127] Берёза Н.В. Киберпреступность // Экономика и социум. 2015. № 1-2 (14). С. 442.

К остальным видам компьютерных преступлений относятся: хищение информации, составляющей коммерческую тайну; использование компьютерных систем для обмена, хранения и распространения информации конфиденциального характера и т.д.

В российском уголовном законодательстве разделение киберпреступлений на определенные группы (составы) отражено в ряде глав Уголовного кодекса РФ и в первую очередь в главе 28 УК РФ, именуемой «Преступления в сфере компьютерной информации» (статьи 272 – 274 УК РФ).

Компьютерные преступления в уголовном законодательстве Российской Федерации.

В статье 272 УК РФ уголовное наказание предусмотрено за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации. Таким образом, предметом преступления является охраняемая законом компьютерная информация. Указанная информация должна находиться на носителе информации (компьютере, мобильном средстве связи) и/или ее программном обеспечении.

В статье 273 главы 28 УК РФ уголовная ответственность предусмотрена за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Такое преступление с объективной стороны проявляется в совершении одного из следующих действий:

– создание компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

– использование таких компьютерных программ или такой компьютерной информации;

– распространение таких компьютерных программ или такой компьютерной информации.

В статье 274 главы 28 УК РФ уголовная ответственность установлена за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации.[128]

Однако, раскрывая шире сферу компьютерной информации, можно отнести также к преступлениям те, в которых присутствуют следующие элементы:

1) компьютерная техника (компьютерная информация) выступает средством (способом) совершения преступления. Рассуждения в данном ключе приводят исследователей к следующим обобщенным выводам: об ошибочности включения в УК РФ главы 28 «Преступления в сфере компьютерной информации», так как научно-

[128] Савиновский А.Н. Преступления в сфере компьютерной информации в законодательстве РФ // Журнал: Экономика, социология и право. 2016. № 5. С. 113.

технический прогресс позволяет совершать все большее количество преступлений путем использования компьютерной техники; о необходимости расширения количества составов преступлений в сфере компьютерной информации в главе 28 УК РФ; о необходимости введения в статьи УК РФ в качестве квалифицирующего признака объективной стороны преступления использования компьютерной техники (компьютерной информации).

2) объективная сторона преступлений заключается либо в распространении (предоставлении) запрещенной или заведомо ложной информации, либо в непредставлении сведений - так называемые информационные преступления.

3) местом или способом совершения преступления является его совершение в информационно-телекоммуникационных сетях.[129]

Многие противоправные посягательства выпадают за пределы действия УК РФ. В этой связи термин «киберпреступления» представляется наиболее адекватно отвечающим сложившейся ситуации. Однако его следует использовать лишь в криминологических целях для обозначения преступности в киберпространстве, которую даже считают формой преступности «белых воротничков». Для обозначения рассматриваемой группы преступлений на законодательном уровне следует использовать термин «преступления в сфере обращения электронной информации».

Помимо изложенного выше, следует отметить, что существует точка зрения, согласно которой использование программно-технических средств или вредоносных компьютерных программ также может рассматриваться как приготовление к совершению преступления, которое по признакам объекта и способа совершения не является информационным.

Тенденции, динамика, прогноз компьютерной преступности в Российской Федерации.

Преступления в информационной сфере сегодня наносят значительный материальный и моральный вред личности, обществу, государству. Анализ состояния, структуры, динамики преступности в сфере высоких технологий позволяет выделить некоторые тенденции и проблемы и сформулировать предложения по ее предупреждению.[130]

По данным отчета о состоянии преступности, ежегодно размещаемого на сайте Министерства внутренних дел, в России отмечается тенденция снижения зарегистрированных преступлений в сфере компьютерной информации: 2010 г. – 7398; 2011 г. – 2698; 2012 г. – 2820; 2013 г. – 2563; 2014 г. – 1739; 2015 г. – 2382.

Так за 2016 год было зарегистрировано 1748 преступлений в сфере компьютерной информации, что на 26,6 % меньше чем за аналогичный период в 2015 году. 1503 преступления было выявлено сотрудниками ОВД. Из преступлений, дела и

[129] Сычев Е.А. Преступления, совершаемые в телекоммуникационных сетях, как разновидность преступлений в сфере компьютерной информации // Журнал: Историческая и социально-образовательная мысль. 2014. № 4 (26). С. 350-355.

[130] Мазуров В.А. Поляков В.В. Криминолого-криминалистическое предупреждение преступности в сфере высоких информационных и телекоммуникационных технологий // Журнал теоретических и прикладных исследований «Известия Алтайского государственного университета». 2009. № 2 (62). С. 95.

материалы о которых находились в производстве, было раскрыто 903 деяния.[131]

И хотя статистические данные свидетельствуют о том, что в последние годы число преступлений в сфере компьютерной информации снизилось, вряд ли их можно связать с совершенством действующего законодательства и успехами правоохранительных органов, скорее, наоборот. Технический прогресс обгоняет теоретическое осмысление происходящего в области создания и применения информационных технологий, использования новых информационно-телекоммуникационных возможностей.

Но такое положение, когда быстро развивающиеся технологии, имеющие тотальный характер, стимулируемые рыночными критериями, слишком долго остаются теоретически неосознанными, чревато непредсказуемыми последствиями.

Последствия в первую очередь выражаются в том, что количество рассматриваемых преступлений и противоправных посягательств в ближайшей перспективе будет только возрастать, что, к сожалению, не обязательно найдет отражение в официальной уголовной статистике и судебно-следственной практике в силу множества причин: дальнейшее развитие IT-технологий и информатизация российского общества, несовершенство уголовного законодательства, недостатки и ошибки в судебно-следственной практике по уголовным делам о преступлениях в сфере компьютерной информации, отсутствие в правоохранительных органах необходимого количества высококвалифицированных специалистов для раскрытия компьютерных преступлений.[132]

Опираясь на представленные сведения о структуре информационной преступности, а также анализируя содержание объекта и способов совершения запрещенных действующим уголовным законодательством преступных деяний, можно прийти к выводу, что к информационным преступлениям в широком смысле, по тому или иному основанию, можно отнести подавляющее число известных современному законодательству преступлений. Фактически информационно-коммуникационные технологии на современном этапе превратились в удобное для многих преступников средство и орудие совершения любого рода преступлений. При этом постоянно расширяющиеся возможности глобальных информационных телекоммуникационных сетей обусловили повышенный интерес к ним со стороны организованной преступности, в том числе экстремистских и террористических организаций. Существующие правила эксплуатации киберпространства позволяют обеспечивать анонимность действий в Сети и существенно осложняют идентификацию пользовательского оборудования.

Основные детерминанты компьютерной преступности. На сегодняшний день, очень много компьютерный преступлений совершается в сфере экономических отношений. Данные, которые хранятся на материальных носителях организаций, предприятий, компаний и фирм стоят очень дорого и могут представлять большую

[131] Министерство внутренних дел: официальный сайт. – URL: http:// мвд.рф (дата обращения: 18.11.2017).
132 Трошин А.А. Противодействие компьютерной преступности как элемент информационной безопасности Российской Федерации // Актуальные проблемы публичного права. 2015. С. 362.

ценность для компьютерных преступников. Как правило, коммерческие взломы осуществляют подготовленные люди, с высоким стажем компьютерных взломов, обладающие специальными познаниями в программировании, шифровании данных, информационной безопасности.[133]

Природу профессиональной компьютерной преступности в сфере экономической деятельности был порожден самим фактом наличия товарно-денежных отношений, то есть: отношений касающихся собственности, материальных благ и потребления. Разделение общества на бедных и богатых, отсутствие среднего класса привели к противоречиям между людьми, установлению неблагоприятного социального климата. Причинами всех этих явлений являются неэффективная экономическая политика, а также несоответствие реальным потребностям общества. Переход к рыночным отношениям активизировал ряд криминальных процессов, которые направлены на поиск путей беспрепятственного обогащения. Психология безудержной наживы формируется на почве массового распространения компьютеров, недостаточной защищенности программного обеспечения и обусловлена минимальным риском разоблачения преступной деятельности. Корыстный мотив компьютерной преступности в экономических отношениях является ключевым в ее механизме, так как создает основу для ее устойчивости, существования киберпреступности как промысла.

Процветанию данного вида преступности также способствует низкий уровень специальной подготовки сотрудников правоохранительных органов, их низкая активность в борьбе с преступлениями в сфере компьютерной информации, а также игнорирование общественной опасности этой категории преступлений со стороны руководства порождают у лиц с неустойчивым уровнем правосознания ощущение полной безнаказанности и провоцируют их к совершению данной категории преступлений. [134]

Таким образом можно выделить следующие условия, способствующие совершению компьютерных преступлений:

1) неконтролируемый доступ сотрудников к пульту управления (клавиатуре) компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе осуществления финансовых операций;

2) отсутствие контроля за действиями обслуживающего персонала, что позволяет преступнику свободно использовать указанную в п. 1 ЭВМ в качестве орудия совершения преступления[135];

3) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

---

[133] Курушин В.Д. Компьютерные преступления и информационная безопасность. М.: Новый юрист, 1998. С. 18.
[134] Максимов В.Ю. Незаконное обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказани : дис. ... канд. юрид. наук. Краснодар, 1998. С. 19.
[135] Вехов В.Б. Компьютерные преступления: Способы совершения, методики расследования. М., 1996. С. 114.

4) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции, ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

5) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации, ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа;

6) отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности, в том числе находящейся в форме машинной информации;

7) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации. Хотелось бы отметить, что условия, способствующие совершению преступлений, во многом создают сами потерпевшие, имеет место неосмотрительность со стороны потерпевших, допускающих посторонних к своим информационным системам без предварительной защиты информации.

В сфере политических отношений.

Политические причины совершения преступлений в сфере компьютерной информации большинством авторов не выделялись в качестве значимых, хотя политические мотивы совершения компьютерных преступлений теоретически допускались некоторыми учеными.

На данный момент ситуация кардинально изменилась, и, по нашему мнению, при анализе причинного комплекса компьютерной преступности в России можно указать на следующие факторы и причины политического характера. Во-первых, это хактивистское движение как политическая причина компьютерной преступности.[136]

Хактивизм (hacktivism от англ. to hack – «рубить» и acktivism – «активизм») предусматривает борьбу за права и свободы личности (свобода слова, свобода информации и т.д.) посредством использования компьютерных технологий и информационно-телекоммуникационных сетей, включая сеть Интернет. Наиболее известными международными хактивистскими движениями являются WikiLeaks и Anonymous.

Считается, что термин был придуман в США (штат Техас) в 1996 г. членом организации Cult of the Dead Cow («Культ мертвой коровы») по кличке Омега.

Протестными формами хактивистского движения является гражданское неповиновение в виде: блокирования правительственных веб-сайтов, перенаправления URL, DDos-атаки, кражи компьютерной информации и демпинга, веб-сайта пародии и т.д. Так, например, российские хакеры из группы Anonymous в марте - мае 2012 г. предприняли DDos-атаки против сайтов СМИ: «Дождь», «НТВ», «Коммерсантъ», «Slon.ru», «Эхо Москвы», а также сайтов Президента и Правительства РФ, заблокировав их на достаточно продолжительное время. Как результат, в январе 2013 г. УФСБ РФ по Красноярскому краю направило в суд уголовные дела в отношении двух жителей г. Красноярска - граждан С. и Х., которые

[136] Осипенко А.Л. Борьба с преступностью в компьютерных сетях. Международный опыт. М., 2004. С.143.

6, 7 и 9 мая 2012 г. при помощи вредоносных компьютерных программ осуществили DDoS-атаки, временно блокировав сайты Президента и Правительства РФ. Действия обвиняемых были квалифицированы по ч. 1 ст. 273 УК РФ, т.е. создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.[137]

Таким образом, хактивистское движение, несмотря на свою политическую направленность и благородную цель «обеспечить свободу информации», без стеснения использует вредоносные компьютерные программы, осуществляя взломы сайтов средств массовой информации, государственных учреждений и органов власти либо с применением уже известного вредоносного программного обеспечения, либо привлекая к сотрудничеству вирусописателей для получения от них новых компьютерных вирусов.

Во-вторых, политическим фактором компьютерной преступности в России, условно назовем его «геополитическим», выступает причинение вреда национальной безопасности Российской Федерации со стороны иных государств, путем использования вредоносного программного обеспечения как информационного оружия для уничтожения или повреждения объектов ее транспортной, энергетической, военной, информационной, финансово-экономической инфраструктуры.[138]

Так называемое «кибероружие» может быть использовано в политических целях для оказания информационного давления или пропаганды путем получения контроля над электронными средствами массовой информации, вывода из строя средств связи и массовых коммуникаций, блокирования объектов энергоснабжения и транспортной инфраструктуры, нарушения производственной деятельности предприятий оборонно-промышленного комплекса, а также причинение вреда иным объектам стратегического значения.[139]

Так, например, в сентябре 2010 г. вирусу Stuxnet удалось проникнуть в компьютеры иранской атомной станции в Бушере и вывести из строя пятую часть центрифуг по обогащению урана, но, к счастью, он не смог вывести из строя основную операционную систему АЭС, что могло привести к катастрофическим последствиям.

Журналистское расследование, проведенное в 2011 г. газетой New York Times, подтвердило предположение «Лаборатории Касперского» и показало, что вредоносная программа Stuxnet была создана спецслужбами Израиля и США для саботажа ядерной программы Ирана.

---

[137] Мелтонян Р.М. К вопросу о сложившихся проблемах выявления и раскрытия преступлений в сфере компьютерной информации и высоких технологий // Журнал «Центральный научный вестник». 2017. № 3 (20). С. 74.

[138] Осипенко А.Л. Борьба с преступностью в компьютерных сетях. Международный опыт. М., 2004. С.149.

[139] Красненкова Е.В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами: дис. … канд. юрид. наук: 12.00.05/Красненкова Елена Валерьевна. М., 2006. 188с.

В апреле 2012 г. обнаружен «таинственный» вирус-троян Wiper, в результате действия которого были уничтожены базы данных в десятках организаций Ирана, при этом больше всего пострадал крупнейший в Иране нефтяной терминал, работа которого была остановлена на несколько дней из-за того, что были уничтожены данные о нефтяных контрактах. Однако не было найдено ни одного образца вредоносной программы, использованной в этих атаках, что многих заставило усомниться в точности сведений, содержащихся в сообщениях СМИ. В процессе расследования таинственной апрельской вредоносной атаки «Лаборатории Касперского» удалось получить и проанализировать образы нескольких жестких дисков, атакованных Wiper. В результате эксперты антивирусной компании подтвердили, что инциденты действительно имели место и что вредоносная программа, использованная в этих атаках, существовала в апреле 2012 г., но после активации Wiper от вредоносной программы не осталось почти никаких следов.

В подтверждение научных тезисов автора можно привести публикацию газеты Washington Post от 01.09.2013, которая со ссылкой на документы, рассекреченные экс-сотрудником ЦРУ Эдвардом Сноуденом, сообщила, что разведывательные службы США в 2011 г. провели 231 кибератаку, направленную против электронных сетей иностранных государств, в том числе России, Китая, Ирана и КНДР.[140]

Третьим политико-информационным фактором компьютерной преступности в России является необходимость получения разведывательными службами иностранных государств конфиденциальной информации геополитического, военно-технического, финансово-экономического, дипломатического и иного стратегического характера о Российской Федерации.

В свою очередь, устранение Российским государством и обществом рассмотренных причин компьютерной преступности должно носить политический, правовой, социально-экономический, организационно-технический, т.е. комплексный характер (совершенствование законодательства, развитие экономики, более качественная подготовка сотрудников правоохранительных органов в сфере информационной безопасности, развитие отечественной электроники и программного обеспечения, привлечение талантливых программистов на государственную службу, правовое просвещение населения и т.д.).

Предупреждение компьютерных преступлений. При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на предупреждение преступления. Меры, направленные на предупреждение преступлений: технические, организационные, правовые.

К техническим мерам относится защита от несанкционированного доступа к системе, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае чрезвычайных ситуаций, установку оборудования обнаружения

[140] Салтевский М.В. Проблемы противодействия преступности в сфере компьютерных технологий // Научно-практическое издание. Москва, 2006.

воды и тушения пожара, принятие конструкционных мер защиты от хищений, диверсий, саботажа, взрывов, установку резервных систем электропитания, оснащение помещений надежными замками, установление сигнализации и др. К организационным мерам можно отнести охрану вычислительного центра, тщательный подбор персонала, наличие плана быстрого восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра, универсальность средств защиты, возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п. К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.[141] Существуют различные способы предотвращения компьютерных преступлений. Но хотелось бы подчеркнуть, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях. В то же время минимизировать риски потерь возможно лишь при комплексном подходе к вопросам безопасности. Кроме того, к специальным правовым мерам предупреждения компьютерных преступлений можно отнести следующие:

1. Совершенствование действующего уголовного законодательства. Например, необходимо законодательное закрепление ряда юридических понятий, содержащихся в диспозициях ст. 272–274 УК РФ, а именно: «компьютерная программа», «несанкционированное уничтожение, блокирование, модификация, копирование компьютерной информации», «нейтрализация средств защиты компьютерной информации», «средства хранения, обработки или передачи охраняемой компьютерной информации», поскольку указанные юридические термины законодательно нигде не определены, а разъяснения Пленума Верховного Суда РФ на данный счет отсутствуют. Следует дополнить гл. 28 УК РФ новыми составами преступлений, например ст. 272.1 «Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации». Данная позиция обусловлена тем, что преступник тайно, открыто или обманным путем завладев, например, флэш-картой или DVD-диском с компьютерной информацией для последующего ее использования, избегает уголовной ответственности по ст. 158, 159, 161 УК РФ в связи с малозначительностью совершенного деяния, так как стоимость вышеуказанных носителей информации не превышает 1 тысячи рублей. При этом виновное лицо получает доступ к компьютерной информации, которая представляет для ее владельца большую ценность, чем сам материальный носитель информации, тем самым потерпевшему причиняется более существенный вред.[142]

---

[141] Пархоменко С.В. Предупреждение компьютерной преступности в российской федерации: интегративный и комплексный подходы // Криминологический журнал байкальского государственного университета экономики и права. 2015. № 2. С. 265.

[142] Трошин А.А. Противодействие компьютерной преступности как элемент информационной безопасности Российской Федерации // Актуальные проблемы публичного права. 2015. С. 362.

Кроме того, для более эффективного противодействия преступлениям в сфере компьютерной информации ряд авторов предлагают дополнить диспозиции ч. 3 ст. 272, ч. 2 ст. 273, ч. 1 ст. 274 УК РФ новыми квалифицирующими признаками:

1) «Те же деяния, совершенные с целью скрыть другое преступление или облегчить его совершение».

2) «Те же деяния, совершенные с целью устрашения населения или воздействия на принятие решения органами государственной власти и (или) местного самоуправления, а также воспрепятствования нормальной деятельности средств массовой информации, органов государственной власти и местного самоуправления, государственных и муниципальных учреждений, предприятий».

При этом рекомендуется установить санкцию за указанные деяния до десяти лет лишения свободы.

Данная позиция обусловлена тем, что преступления в сфере компьютерной информации часто выступают или могут стать способом совершения множества других тяжких и особо тяжких преступных деяний (убийства, причинения тяжкого вреда здоровью, умышленного уничтожения или повреждения имущества, вымогательства, шпионажа, государственной измены и т.д.).

При этом полагаем возможным внести изменения в ст. 151 УПК РФ в плане отнесения преступлений, предусмотренных ч. 2–4 ст. 272, ч. 2, 3 ст. 273, ч. 1, 2 ст. 274 УК РФ к подследственности органов ФСБ РФ, поскольку вышеуказанные преступные деяния, безусловно, представляют угрозу национальной безопасности Российской Федерации.[143]

2. Совершенствование судебной практики по уголовным делам о компьютерных преступлениях в Российской Федерации.

До сих пор отсутствуют разъяснения Пленума Верховного Суда РФ о практике рассмотрения судами уголовных дел по преступлениям в сфере компьютерной информации, что негативно сказывается на следственно-судебной практике и единообразии применения уголовно-правовых норм правоохранительными органами.[144]

Кроме того, в подавляющем большинстве случаев суды при вынесении обвинительных приговоров назначают компьютерным преступникам наказания, не связанные с лишением свободы (штраф, условное наказание, ограничение свободы и др.), обосновывая свое решение тем, что данные преступления относятся к деяниям небольшой и средней тяжести.

Кроме того, совершенствование судебной практики требует разъяснений Пленума Верховного Суда РФ по вопросам квалификации деяний, предусмотренных ст. 272–274 УК РФ.

Например, будет ли являться уничтожением компьютерной информации деяние,

---

[143] Пархоменко С.В. Предупреждение компьютерной преступности в российской федерации: интегративный и комплексный подходы // Криминологический журнал байкальского государственного университета экономики и права. 2015. № 2. С. 265-276.

[144] Гулян, А.Р. Основные направления противодействия компьютерной преступности в Российской Федерации // Российский следователь. 2009. № 5. С. 27-29.

при котором информация была изначально уничтожена, но спустя определенное время частично или полностью восстановлена специалистами? Как квалифицировать уничтожение компьютерной информации сильным электромагнитным или высокочастотным излучением, не повлекшим уничтожение самого носителя информации? Будут ли являться копированием компьютерной информации действия преступника при получении копии документа путем распечатывания информации на принтере, фотографирования или видеосъемки изображения с монитора компьютера?

Наконец, как квалифицировать несанкционированное ознакомление с компьютерной информацией, когда преступник, визуально запомнив конфиденциальные сведения (например, персональные данные лица, информацию о содержании коммерческой сделки и сторонах договора, сведения об усыновлении (удочерении), врачебную тайну и т.д.), впоследствии переносит их на другой материальный носитель информации, создав ее копию (написав на листе бумаги, введя информацию в память своего компьютера или иного компьютерного устройства -айфона, смартфона, планшетного компьютера, коммуникатора и т.п.).

3. Активизация и совершенствование международно-правового сотрудничества в сфере предупреждения компьютерных преступлений и борьбы с ними.

Учитывая транснациональный и трансграничный характер рассматриваемых преступлений, большое значение приобретает вопрос взаимодействия правоохранительных органов России и зарубежных стран в сфере противодействия компьютерной преступности.

В наши дни жертвами преступлений в сфере информационных технологий становятся не только руководители высшего звена и правительственные организации, но и простые граждане.

В связи с этим возникает вполне логичный вопрос о фактическом состоянии (количестве и качестве) совершаемых в Российской Федерации преступлений в сфере компьютерной информации и высоких технологий, об их официальной государственной регистрации и латентном характере деяний в указанной сфере. Отдельно – вопрос об уровне профессиональной подготовленности сотрудников правоохранительных органов, социализирующихся на выявлении, раскрытии и расследовании названных преступлений.[145]

На сегодняшний день ключевой проблемой в сфере киберпреступлений являются недостаточная «техническая подкованность» оперативных сотрудников и следователей. Так, около 90 - 95 % из них имеют высшее юридическое образование, и только 5-10 % получили второе техническое образование по следующим специальностям: 02.00.00 – компьютерные и информационные науки, 09.00.00 – информатика и вычислительная техника, 11.00.00 – электроника, радиотехника и системы связи.

Исходя из этого киберпреступники по-прежнему технически грамотнее

[145] Салтевский М.В. Проблемы противодействия преступности в сфере компьютерных технологий // Научно-практическое издание. Москва, 2006.

сотрудников полиции (юстиции), поскольку даже те сотрудники, которые имеют техническое образование не всегда обладают достаточными знаниями и практическим опытом для выявления и раскрытия преступлений в сфере компьютерной информации и высоких технологий. Например, определить IP – адрес (уникальный сетевой адрес узла в компьютерной сети, построенный по протоколу IP) лица, который можно передать провайдеру с целью установления местонахождения (адреса проживания) пользователя услуг интернета – преступника.[146]

Как следствие появление другой проблемы, связанной с несвоевременностью выявления и раскрытия киберпреступлений. Так в 49 % случаев с момента реализации преступного умысла в сети интернет и до поступления в полицию информации о совершенном преступлении проходит свыше 10 суток. В 84 % случаев срок проверки сообщения о совершении преступления в сфере компьютерной информации и высоких технологий продлевается до 10 и 30 суток, в том числе по причине отсутствия на местном (районном) уровне специалистов способных правильно оценить событие преступления. В итоге имеет место факт несвоевременного (запоздалого) начала предварительного расследования, когда значительная часть важных доказательств была утрачена, в том числе по вине потерпевшего, пытавшегося самостоятельно решить сложившуюся ситуацию.

Организационно – исполнительные меры предупреждения компьютерной преступности.

К специальным организационно-управленческим и техническим мерам предупреждения компьютерных преступлений можно отнести следующее:

1. Подготовка специалистов по специальностям «Информационная безопасность», «Защита информации и информационно-телекоммуникационных сетей» в высших учебных заведениях МВД, ФСБ, МО, ФТС РФ и др. с целью дальнейшего комплектования правоохранительных органов профессиональными и компетентными сотрудниками.

2. Требуется тесное взаимодействие органов прокуратуры, органов внутренних дел (отделов «К»), органов Федеральной службы безопасности со средствами массовой информации при предупреждении и раскрытии преступлений в сфере компьютерной информации. Анализ правоприменительной практики показывает эффективность такого взаимодействия, тем более что основные формы сотрудничества правоохранительных органов и средств массовой информации давно уже апробированы и активно используются.

3. Создание в Российской Федерации национальной операционной системы для компьютерных устройств, а также общенациональной компьютерной системы фиксации, анализа и учета преступлений в сфере компьютерной информации и компьютерных преступников (разработку таких систем можно поручить российским компаниям: «Лаборатория Касперского», Dr. Web, Group-IB).

---

[146] Мелтонян Р.М. К вопросу о сложившихся проблемах выявления и раскрытия преступлений в сфере компьютерной информации и высоких технологий // Журнал «Центральный научный вестник». 2017. № 3 (20). С. 74.

В данное время системная подготовка экспертов-криминалистов и повышение их квалификации при проведении судебно-компьютерных экспертиз в системе МВД России не осуществляется, поэтому возникает необходимость создания единого учебного центра на базе ЭКЦ МВД РФ либо одного из образовательных учреждений МВД России, имеющих необходимый опыт обучения экспертов-криминалистов.[147]

Перечень мер по предупреждению компьютерной преступности может быть продолжен. Однако, вне всякого сомнения, только комплексный подход в применении правоохранительными органами профилактических мер может повысить уровень информационной безопасности России и сделать предупреждение компьютерных преступлений более эффективным. При этом не стоит забывать, что предложенные меры дадут ощутимый результат только в случае совместных действий государства с органами местного самоуправления, образовательными и научными учреждениями, средствами массовой информации, общественными объединениями и т.д.

Подводя итог вышесказанному можно сделать вывод о том, что выявление, раскрытие и расследование преступлений в сфере компьютерной информации и высоких технологий, по-прежнему остается одной из труднейших задач для уголовного розыска и органов предварительного расследования. Это, безусловно связано с целым рядом проблем, среди которых выделяются такие из них как отсутствие должного мониторинга следственной и судебной практики в области киберпреступлений, в целом не значительным опытом работы, подготовкой следователей и сотрудников уголовного розыска, которые ранее не сталкивались с подобными преступлениями, наконец, общая нехватка научно обоснованных и апробированных на практике методических рекомендаций по тактике и методике расследования преступлений в сфере компьютерной информации и высоких технологий.

Заключение. Сегодня компьютерные технологии плотно вошли в нашу жизнь. С каждым годом, компьютеризация населения становятся все выше. Это связано с развитием и удешевлением производства технологичных устройств, а также быстрым внедрением их в массы. И именно виртуальная площадка, входом на которую служит компьютер и иные портативные устройства становится оружием для совершения преступлений, которые влекут за собой тяжкие последствия экономического, политического и личного характера.

Исследовав компьютерные преступления в разных сферах жизни общества, можно сделать следующие выводы:

1) Использование программно-технических средств или вредоносных компьютерных программ также может рассматриваться как приготовление к совершению преступления, которое по признакам объекта и способа совершения не является информационным. Опираясь на представленные сведения о структуре

[147] Пархоменко С.В. Предупреждение компьютерной преступности в российской федерации: интегративный и комплексный подходы // Криминологический журнал байкальского государственного университета экономики и права. 2015. № 2. С. 273.

информационной преступности, а также анализируя содержание объекта и способов совершения запрещенных действующим уголовным законодательством преступных деяний, можно также прийти к выводу, что к информационным преступлениям в широком смысле, по тому или иному основанию, можно отнести подавляющее число известных современному законодательству преступлений. Причем данный вывод можно распространить и на структуру киберпреступности;

2) Основными условиями компьютерных преступлений является:

– неконтролируемый доступ сотрудников к пульту управления (клавиатуре) компьютера;

– отсутствие контроля за действиями обслуживающего персонала

– низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

– несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции;

– отсутствие должностных лиц, отвечающего за режим секретности и конфиденциальности информации;

– отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности, в том числе находящейся в форме машинной информации.

Хотелось бы отметить, что условия, способствующие совершению преступлений, во многом создают сами потерпевшие, имеет место неосмотрительность со стороны потерпевших, допускающих посторонних к своим информационным системам без предварительной защиты информации.

В свою очередь, устранение российским государством и обществом рассмотренных причин компьютерной преступности должно носить комплексный характер (совершенствование законодательства, развитие экономики, более качественная подготовка сотрудников правоохранительных органов в сфере информационной безопасности, развитие отечественной электроники и программного обеспечения, привлечение талантливых программистов на государственную службу, правовое просвещение населения и т.д.).

Исходя из этого киберпреступники по-прежнему технически грамотнее сотрудников полиции (юстиции), поскольку даже те сотрудники, которые имеют техническое образование не всегда обладают достаточными знаниями и практическим опытом для выявления и раскрытия преступлений в сфере компьютерной информации и высоких технологий.

Подводя итог вышесказанному можно сделать вывод о том, что раскрытие и расследование преступлений в сфере компьютерной информации и высоких технологий, по-прежнему остается одной из труднейших задач для уголовного розыска и органов предварительного расследования. Это, безусловно связано с целым рядом проблем, среди которых выделяются такие из них как отсутствие должного мониторинга следственной и судебной практики в области киберпреступлений, в

целом не значительным опытом работы, подготовкой следователей и сотрудников уголовного розыска, которые ранее не сталкивались с подобными преступлениями, наконец, общая нехватка научно обоснованных и апробированных на практике методических рекомендаций по тактике и методике расследования преступлений в сфере компьютерной информации и высоких технологий.

ИСТОРИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННЫХ ВОЙН В СОВРЕМЕННОЙ РОССИИ (Бедарева А.А., Чудаева Д.К.)

Понятие и общая характеристика информационных войн. «Информационная война» — термин, безусловно, важный и актуальный на современном этапе развития общества, без четко понимания которого нельзя понять процессы, происходящие в современной политической жизни и геополитике.

В докладе Генерального секретаря ООН (A/56/164МШ.1 от 3 октября 2001 г.) информационные войны были отнесены к основным угрозам личности, обществу и государству в информационном пространстве наряду с такими угрозами, как разработка и использование средств несанкционированного вмешательства в информационную сферу другого государства; неправомерное использование чужих информационных ресурсов и нанесение им ущерба; целенаправленное информационное воздействие на население иностранного государства; попытки доминирования в информационном пространстве; поощрение терроризма.

Впервые термин «информационная война» был употреблен Т. Рона в отчете «Системы оружия и информационная война», подготовленном им в 1976 г.. Он подчеркивал, что информационная инфраструктура является ключевым аспектом американской экономики, в то же самое время она становится и уязвимой целью как в военное, так и в мирное время.

По мнению И. Н. Панарина, за точку отсчета следует принять не 1976 г., а 1967 г., когда А. Даллес (главный организатор информационной войны против Советского Союза) выпустил книгу под названием «Тайная капитуляция», посвященную тайным сепаратным переговорам между США и Великобританией, с одной стороны, и рейхсфюрером СС Гиммлером — с другой. В ней впервые вводился термин «информационная война», представляющий собой личные, разведывательные, диверсионные действия по подрыву тыла противника . Позднее этот термин стал активно упоминаться в прессе, особенно после проведения в 1991 г. операции «Буря в пустыне».

В настоящее время понятие «информационная война» определяется по-разному. Это связано с многозначностью термина «information warfare», что породило множество разночтений при его переводах. Он может трактоваться как «информационная война», «информационное противоборство», «информационно-психологическая война». В частности, информационная война характеризуется как информационная деятельность, предпринимаемая политическим образованием (например государством) для ослабления, уничтожения другого политического образования; как информационная борьба между соревнующимися конкурентами; информационный военный конфликт между двумя массовыми врагами, например армиями и т. п.

При выявлении сущности информационной войны прежде всего выделяют трактовки, в которых этот термин относится к сфере военного противоборства. В октябре 1998 г. в США была введена в действие Объединенная доктрина информационных операций, в которой под информационной войной понимается комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника. Одновременно с наступательным воздействием информационное противоборство предполагает обеспечение надежной защиты национальной информационной инфраструктуры США.

Как отмечают американские военные эксперты, информационная война состоит из действий, предпринимаемых для достижения информационного превосходства в интересах национальной стратегии и осуществляемых путем влияния на информацию и информационные системы противника при одновременной защите собственной информации и своих информационных систем. При этом информационное превосходство определяется как способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать то же самое.

Аналогичной точки зрения придерживается С. А. Комов. В военное время информационная война включает «комплекс информационной поддержки, информационных контрмер, мер информационной защиты, предпринимаемых в соответствии с единым планом и нацеленных на достижение и поддержание информационного превосходства над противником во время боевых действий». По его мнению, для вооруженных сил понятие информационной войны имеет следующие аспекты: определение мер для получения информации о противнике и условиях боя (например, погода, инженерное оборудование и т. д.), для сбора информации о своих и взаимодействующих войсках; определение мер по блокированию процесса сбора противником информации о войсках, планирование мер по дезинформации на всех этапах боевых действий; осуществление мероприятий по организации взаимодействия с другими воинскими контингентами, участвующими в конфликте и т. д.

В рамках этого подхода необходимо упомянуть точку зрения С. П. Расторгуева, акцентирующего внимание на том, что информационная война — это открытые и скрытые целенаправленные информационные воздействия информационных систем друг на друга с целью получения определенного выигрыша в материальной сфере.

Данный аспект подчеркивался и специалистами МИД России, которые отмечали, что информационная война — это «противоборство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным структурам, подрыва политической, экономической и социальной систем, а также массированной

психологической обработки населения с целью дестабилизации общества и государства».

Вторая группа определений трактует информационную войну как форму геополитического противоборства. Так, Л. Г. Ивашов информационное противоборство определяет как совокупность отношений информационной защиты и информационного соперничества противостоящих геополитических субъектов.

Анализируя современный этап развития, авторы, например В. Дергачев, констатируют, что глобальная система Интернета превращается в фактор политической и экономической действительности, в средство геополитической коммуникации, где мобильность информации становится стратегическим ресурсом, не имеющим территориально-государственной организации. Автор отмечает появление такого нового «поля боя» информационных войн, как киберпространство. Информационно-технологическая составляющая, по его мнению, внесла существенные коррективы в геополитику. В этой связи современная геополитическая мощь государства определяется не материальными ресурсами, а силой духа. Новейшая геополитика оперирует «большими» пространствами многомерной сопряженности, включая виртуальное пространство Всемирной сети (киберпространство) и вооружена информационно-коммуникационными технологиями манипулирования сознанием, позволяющими эффективно вести сетевые войны.

В широком плане информационная война рассматривается И. Василенко, которая определяет ее «как планомерное информационное воздействие на всю инфокоммуникационную систему противника и нейтральные государства с целью формирования благоприятной глобальной информационной среды для проведения любых политических и геополитических операций, обеспечивающих максимальный контроль над пространством».

Кроме того, информационная война может пониматься как новая форма борьбы двух и более сторон. По мнению В. С. Пирумова, она состоит в целенаправленном использовании специальных средств и методов влияния на информационные ресурсы противника, а также защиты собственного информационного ресурса для достижения назначенных целей. Автор отмечает, что в мирное время информационная война носит преимущественно скрытый характер, и ее основное содержание — ведение разведывательных и политико-психологических действий по отношению к противнику, осуществление мероприятий по собственной информационной безопасности.

Анализируя литературу, на мой взгляд, нужно акцентировать внимание на одном важном вопросе: можно ли ставить знак равенства между информационной войной и информационным противоборством? Так, выше отмечалось, что информационная война может трактоваться как противоборство. Однако не все авторы соглашаются с этим. В частности, И. Н. Панарин настаивает на том, что «информационное противоборство — это форма борьбы сторон, заключающаяся в воздействии на информационную среду противостоящей стороны и защите собственной от

негативных информационных воздействий. Отличие этих двух понятий лишь в том, что информационная война производится более активно с использованием диверсионных и террористических методов».

Другой точки зрения придерживается А. В. Манойло. По его мнению, «информационная война» и «информационное противоборство», по существу, одно и то же. Термин «информационно-психологическая война» на российскую почву перенесен из словаря военных кругов США и дословно означает «information and psychological warfare» и поэтому может звучать как «информационное противоборство», так и «информационная психологическая война» в зависимости от контекста. В то же время им предлагается определение информационной войны, которое созвучно мнению И. Н. Панарина — это наиболее социально опасная форма информационного противоборства, осуществляемая насильственными средствами и способами воздействия на информационно-психологическую сферу противника с целью решения стратегических задач.

В этой связи выделяется ряд трактовок, в которых информационная война может рассматриваться как информационно-психологическая. В частности,

В. Лисичкин и Л. Шелепин под информационно-психологической войной понимают войну нового типа, «в которой используется канал непосредственного воздействия на общественное сознание, на души людей. Задача состоит в том, чтобы заставить массы действовать в нужном направлении даже против своих интересов, а в стане противника расколоть людей, заставить их встать друг против друга».

С. А. Зелинский также акцентирует внимание на том, что психологическая война, в отличие от войн, в которых задействуется военная техника, происходит информационным способом, оказывающимся в результате значительно эффективней по охвату аудитории и не причинении разрушений материальных средств. Поэтому эти понятия не следует отделять, так как информация является основным двигательным механизмом ведения психологических войн.

В этой связи заслуживает внимания точка зрения А. В. Манойло, определяющего информационно-психологическую войну как боевые действия, спланированные в соответствии с пиар-сценарием, цель которых — не уничтожение живой силы и техники противника, а достижение определенного пиар-эффекта. Продукт современной операции информационно-психологической войны — это сводка новостей СМИ в формате журналистского репортажа . в силу чего происходит формирование нужного общественного мнения. В итоге можно изменить жизнь человека, а если потребуется и способ существования, в том числе и социальный уклад населения, общественный строй.

В информационной войне существуют три основные цели: контроль информационного пространства и обеспечение защиты своей информации от вражеских действий; использование контроля над информационным пространством для проведения информационных атак на врага; повышение общей эффективности вооруженных сил путем повсеместного внедрения военных информационных функций.

В качестве составных частей информационной войны выделяют: психологические операции с целью воздействия на мотивацию военнослужащих противника; дезинформация – предоставление противнику ложной информации о наших силах и планах; радиоэлектронная война, заключающаяся в «ослеплении» вражеских систем радиоэлектронной разведки; физическое разрушение элементов информационных системы противника; информационная атака – разрушение или искажение информации без видимых повреждений носителя; защита своей информации.

Существует два вида информационных атак: косвенная и прямая. Разницу между ними лучше всего пояснить на примере. Допустим, мы хотим ввести командование противника в заблуждение относительно места дислокации нашей авиационной части. Можно построить ложный аэродром, разместить там макеты самолетов и имитировать деятельность по их техническому обслуживанию. Это – косвенная информационная атака. А можно внедрить ложную информацию о местонахождении той же авиационной части прямо в хранилище информации противника, чтобы при принятии решений вражеское командование оперировало ложными данными. Это – прямая информационная атака. Таким образом, по своему характеру информационная война занимает положение между «холодной» войной, включающей, в частности, экономическую, и реальными боевыми действиями с участием вооруженных сил. В отличие от экономической, результатом информационной войны является нарушение функционирования элементов инфраструктуры противника (пунктов управления, ракетных и стартовых позиций, аэродромов, портов, систем связи, складов и т. д.), а в отличие от «горячей» войны с применением обычных вооружений и (или) оружия массового поражения ее целями являются не материальные, а «идеальные» объекты (знаковые системы) или их материальные носители. В то же время разрушение таких объектов и систем может осуществляться с сохранением их материальной основы. Роль информационной войны сегодня осознается и российским военно-политическим руководством. В выступлении вице-премьера и председателя Военно-промышленной комиссии РФ Дмитрия Рогозина в «Российской газете», сделанном 28 июня 2013 года, говорится следующее: «Если раньше все военные наработки в этой сфере [кибероружия] затрагивали лишь обеспечение безопасности компьютерных систем и коммуникаций, то теперь информационные технологии рассматриваются как оружие первого удара. В случае конфликта с каким-либо государством, возможная первая атака производится через информационные сети, в ходе которой разрушаются критически важные объекты инфраструктуры государства, нарушается система политического и военного управления, выключаются станки с электромозгами, основанными на импортной электронно-компонентной базе. Когда же государство-жертва агрессии становится практически парализованным, наносится удар классическими военными средствами».

Виды информационной войны. Информационная война может применяться среди военных и среди мирного населения. Для этого может использоваться один из видов

информационной войны или комплекс мероприятий. К видам информационного противостояния относятся:

Информационная война в интернете - предлагается разная и зачастую противоречивая информация, применяемая для запутывания противника.

Психологические операции – подбор и подача такой информации, которая звучит как контраргумент на настроения, существующие в обществе.

Дезинформация – продвижение ложной информации с целью направления вражеской стороны по неправильному следу.

Разрушение – физическое уничтожение или блокировка электронных систем, важных для противника.

Меры безопасности – усиление охраны своих ресурсов с целью сохранения планов и намерений.

Прямые информационные атаки – смешение ложной и правдивой информации.

Ретроспективный анализ информационных войн. Мировое информационное пространство в XXI веке заполнено информационными войнами. С каждым годом их количество растет и уже термин «информационная война» воспринимается без удивления и становится обычным явлением во время как внутригосударственного, так и международных конфликтов. Многие предполагают, что информационные войны пришли к нам только в XX веке, вместе с эрой технологий, но это не так.

Один из первых случаев применения информационно-психологического влияния относится ещё к V веке до н. э., когда персидский царь Ксеркс I, пытаясь устрашить эллинов, распространял слухи о гигантских размерах своей армии.

Упоминание об информационных войнах, встречается у Сунь Цзы в «Трактате о военном искусстве». Как свидетельствуют исследования зарубежных ученных, этот трактат был написан полководцем и стратегом в IV веке до н. э. (приблизительно 380-325 годы до н. э.). В трактате выделяется один из важных методов психологического влияния во время войны, а именно дезинформация, обман. Он писал: «Война — это путь обмана. Поэтому, если ты и можешь что-нибудь, показывай противнику, будто не можешь; если ты и пользуешься чем-нибудь, показывай ему, будто ты этим не пользуешься...» .

Нельзя оставить без внимания и важный памятник права стран Древнего Востока — свод древнеиндийских законов Ману. Их составление относят ко II в. до н. э. — I в. н. э. Согласно этим Законам Ману, войска противника следует поощрять к мятежу, внося раскол в ряды тех, кто к этому склонен. Этим принципом пользовались многие стратеги античности, средневековья и нового времени .

Так в итальянских и австрийских компаниях в 1804-1807 гг. Наполеон Бонапарт умело использовал газеты и корреспондентов нейтральных государств (Швейцария, Англия) для распространения дезинформации про расположения собственных войск.

В XX веке информационные войны стали частью военной политики государств. Например, в Первую мировую войну в Великобритании было создано так называемое Бюро военной пропаганды (1914 г.), которое позже переименовано в Управление военной информации. Во Франции при втором отделе генерального штаба

министерства обороны был создан отдел Службы военной пропаганды (1915 г.). Оба учреждения занимались распространением пропаганды среди военных и гражданских лиц других государств. В 1917 г. США создали психологическую секцию при разведслужбе штаба экспедиционных войск. Основными средствами ведения информационной войны в то время были листовки, открытки, газеты; в качестве технических средств русской армией использовались громкоговорители.

Сразу после Первой мировой войны вырос интерес к этому явлению. Во многих государствах мира стали появляться работы по психологическим методам ведения войны. Английский исследователь психологической войны П. Г. Уорбертон писал: «В современное время основной задачей в войне является не уничтожение вооруженных сил противника, как это было раньше, а подрыв морального состояния населения вражеской страны в целом до такого уровня, чтобы оно заставило свое правительство пойти на мир. Вооруженное столкновение армий — это лишь одно из средств для достижения этой цели».

Таким образом, теория информационной и психологической войны стала разрабатываться уже во время и после Первой мировой войны. До Второй мировой войны существовала активная пропаганда режимов: в Германии 19331941 гг. — нацистская пропаганда, в СССР — коммунистическая и антикапиталистическая, в США и Великобритании — капиталистическая и антикоммунистическая. Во время Великой Отечественной войны акценты быстро сдвинулись в сторону антинацистской пропаганды.

В это время уже функционировали органы государственной пропаганды. В СССР это были Бюро военно-политической пропаганды и 7-е управление ГлавПУР РККА. В нацистской Германии работали Министерство народного просвещения и пропаганды и Верховное главнокомандование Вермахта. Свои органы пропаганды существовали в США и Великобритании. Во время войны применяемые методы психологического воздействия часто имели высокую эффективность. Несмотря на развитие информационных технологий в то время, по-прежнему больше всего пропаганды существовало в виде листовок и плакатов. Активно применялось также радиовещание на языке противника.

После Второй мировой войны теория психологической войны обогатилась. На фоне противоборства СССР и США во время Холодной войны, а также в локальных войнах, происходивших в это время, информационные войны стали приобретать новые очертания. Так, в 1950 году в США создано Управление психологической войны, которое вело пропагандистскую войну (в том числе при помощи так называемых «агитационных снарядов») во время Корейской войны. В свою очередь, пропагандистские органы Корейской народной армии и Народно-освободительной армии Китая при поддержке аппарата пропаганды Вооружённых сил СССР производили масштабное психологическое воздействие на военных Южной Кореи и США, причём более успешное.

Результаты Корейской войны были критически переосмыслены в США, и уже в 1955 году принято новое положения «Ведение психологической войны», в котором

подчёркивалось: «Психологическая война включает мероприятия, при помощи которых передаются идеи и информация для оказания влияния на сознание, чувства и действия противника. Они проводятся командованием в сочетании с боевыми операциями в целях подрыва морального духа противника в соответствии с политикой, провозглашённой руководящими инстанциями». Управление психологической войны было переименовано в Управление специальных методов войны, назначение которого обосновал генерал У Троскел: «Специальные методы войны — это соединение приемов, форм и методов психологической войны с другими средствами, направленными на подрыв противника изнутри. Они расширяют поле боя и превращаются из временно действующего тактического средства ограниченного воздействия в мощное стратегическое оружие, имеющее большие потенциальные возможности».

Органы пропаганды США применяли новые наработки во время войны во Вьетнаме. Помимо жестоких чисток американскими войсками вьетнамских деревень и городов, они активно внедряли технологии внушения страха у населения и военных, используя все знания о культуре и суевериях вьетнамцев. Информационно-психологическая обработка деморализовала армию противника и предшествовала физическому уничтожению. Во время этой войны были первые попытки использовать телевидение в качестве средства распространения пропаганды, также предпринимались попытки создания компьютерных баз данных для накопления и обработки информации и информационную систему РЛМБ. Поражение США во Вьетнамской войне способствовало очередному пересмотру тактики и стратегии ведения информационно-психологической войны.

Война в Афганистане 1979-1989 гг. стала ещё одной возможностью для США применить свои технологии, однако американские агенты не принимали масштабного участия в военных действиях, а исподтишка спонсировали моджахедов, давая им оружие и натравливая на советских военных, распространяя вымышленные слухи об их преступлениях против афганских детей. Советская пропаганда в Афганистане была намного «гуманнее» и предполагала распространение политических анекдотов об оппозиционных лидерах. Основная же тактика советских войск сводилась к материальной поддержке афганцев для предотвращения диверсий и для их расположения. Оказывалась медицинская помощь, практиковалась бесплатная раздача керосина.

Во время войны в Персидском заливе в 1991 г. в Эр-Рияде коалицией многонациональных сил была создана специальная рабочая группа, которая отвечала за проведение «психологических операций». Особенно эффективными методами ведения войны стали листовки и радиовещание. По итогам войны признано, что иракская армия была почти полностью деморализована, даже не принимая участия в боях.

Информационная война в XX веке часто сопровождала реальные военные конфликты, являясь их составной частью. В XXI веке уже можно говорить об

«информационном противостоянии», являющемся частью политического противостояния как в мирное время, так и на фоне войны.

Учитывая высокий авторитет, к ведению информационной войны в прошлом нередко подключали церковь. Так, например, во время войны 1812 году католик Наполеон был дважды предан анафеме московской православной церковью, о чем было объявлено российским подданным. Правда, между отлучениями он был награжден высшей наградой империи – орденом Андрея Первозванного.

С появлением книгопечатания и постепенного проникновения грамотности в широкие массы в информационной войне все чаще стали использовать печатное слово. Так началась информационная война в СМИ. Типичным носителем пропаганды и дезинформации стала листовка, их разными способами доставляли до вражеских солдат или населения. В «промышленных» масштабах использование листовок началось во время Первой мировой войны. В этот же период основные участники конфликта создали специальные службы, которые занимались пропагандой.

Вообще, следует сказать, что именно Первая мировая война дала небывалый толчок развитию информационных средств ведения войны. После окончания этого конфликта значительное число исследователей занялось разработкой теоретической базы психологической войны. Впервые появилось определение, что целью войны является не уничтожение армии противника, а подрыв морального состояния всего населения государства-противника до такой степени, чтобы оно заставило свое правительство капитулировать.

Удивительно, но Первая мировая война четко показала, что пропаганда в первую очередь должна быть направлена против собственного населения и армии. Лучшими пропагандистами ПМВ были англичане. Кроме всего прочего, они первыми додумались до создания агитснарядов, агитмин и даже винтовочных агитгранат.

Одной из блестящих технологий информационной войны, которую вероломные англосаксы применяли против немцев, стала так называемая пропаганда ужасов. В самых известных газетах печатали полностью фейковые материалы о жестокостях и зверствах германских войск: насилии над монашками, казнях священников, жестоких убийствах пленных британских солдат. Типичным примером фейка того времени является история распятого канадского солдата, так что сюжет Первого российского канала о «распятом славянском мальчике» — это унылый плагиат с некоторой добавкой треша.

Самой гнусной выдуманной историей того времени является английский фейк о том, что немцы перерабатывают трупы своих и чужих солдат для корма свиней. Она вызвала целую бурю негодования во всем мире: после этой новости Китай присоединился к Антанте, а в самой Англии и в Америке материал вызвал небывалый наплыв добровольцев, желающих отправиться на фронт. Мол, как же это так, братцы? Кормить павшими джентльменами свиней? Давайте-ка надерем задницы этим гнусным тевтонам.

Следует отметить, что материалы были отлично сфабрикованы – все факты подтверждали подготовленные свидетели, и люди действительно верили в них.

Немцы также пытались провернуть что-то подобное: они рассказывали своему населению, что русские казаки едят младенцев (им опять же верили). Это заставляло германских солдат на фронте сражаться еще более героически, дабы защитить Фатерлянд от диких азиатских людоедов.

Еще одним направлением английской пропаганды ПМВ было преуменьшение собственных потерь и преувеличение военных достижений. Естественно, что солдаты Антанты изображались в газетах в качестве благородных и бесстрашных рыцарей.

Руководил британской пропагандой во время Первой мировой войны лорд Нортклифф. Можно сказать, что этот человек поднял информационную войну на совершенно новый уровень. Сегодня каждый грамотный человек знает фамилию гитлеровского министра пропаганды Геббельса. Однако, не вызывает сомнения, что этот злой гений Гитлера имел очень хороших учителей и уже проверенные методики по превращению среднестатистического гражданина в убийцу и чудовище.

Нельзя сказать, что лорд Нортклифф открыл что-то совсем новое: во все времена собственных солдат изображали героями, а вражеских — убийцами и злодеями. Однако пропагандисты ПМВ получили в свои руки новый мощный инструмент – средства массовой информации, – которые могли донести идеи пропагандистов до основной массы к тому времени уже грамотного населения. Англичанам оставалось доработать всего лишь «незначительные» детали: решиться на создание абсолютно трешевых и полностью выдуманных материалов, научиться готовить подставных свидетелей и фабриковать фотографии своих ужасов. И поставить все вышеперечисленное на конвейер.

Кстати, немцы во время ПМВ так и не решились на такое (зато они по полной отыгрались во время следующей мировой бойни). Позже будущий фюрер Третьего Рейха Адольф Гитлер в своей книге Mein Kampf написал следующее: «Чем чудовищнее солжёшь, тем скорее тебе поверят. Рядовые люди скорее верят большой лжи, чем маленькой… Большая ложь даже просто не придёт им в голову. Вот почему масса не может себе представить, чтобы и другие были способны на слишком уж чудовищную ложь…»

Во время Второй мировой войны все участники конфликта уделяли информационной войне огромное значение. Этим вопросом занимались специальные структуры, пропаганда велась как среди собственного населения и армии, так и среди войск и населения противника. Особенностью этого конфликта стала еще большая роль средств массовой информации, появилось радио и кинематограф. Для продвижения дезинформации на территории Британии немцы умудрились создать даже несколько фейковых радиостанций, которые, якобы, находились в Англии, и имели стиль вещания похожий на английские ресурсы. Через них регулярно «вбрасывалась» дезинформация, направленная на деморализацию английского общества.

Похожими вещами занимались и англичане.

Не забывали и более традиционные методы воздействия: над вражеской территорией и позициями войск разбрасывались листовки или пропуски для сдачи в плен. Советские пропагандисты на фронте активно использовали громкоговорители, через которые к немецким солдатам часто обращались пленные, призывая своих товарищей сдаться.

Новое развитие информационные методы ведения боевых действий получили в эпоху Холодной войны. Это было время столкновения двух идеологических систем: западной и советской. Однако после двух мировых войн пропаганда несколько изменилась. Американские специалисты психологической войны высказали это таким образом: «Пропаганда практически только тогда обречена на провал, если она внешне похожа на пропаганду».

Американцы весьма активно и довольно успешно использовали методы психологической войны во Вьетнаме. Основной упор делался на деморализацию и запугивание местного населения и бойцов партизанских отрядов. За время боевых действий им удалось добиться перехода на свою сторону более 250 тыс. вьетнамцев.

СССР оттачивал методы ведения психологической войны в Афганистане. Проводились самые разные агитационно-пропагандистские мероприятия, от раздачи материальной помощи до распространения слухов и анекдотов про главарей моджахедов. Однако, следует отметить, что советские войска в афганской войне уделяли пропаганде намного меньше внимания, чем США во Вьетнаме.

Информационные войны в современной России. Открытым началом текущего витка информационной войны можно считать 1953 год, когда американцы запустили проект «Радио Свобода», служивший для идеологической поддержки советских диссидентов. Собственно, именно американцы и возглавили информационный крестовый поход против СССР.

Планы широкомасштабной информационной войны появились в Великобритании и США ещё раньше:

• Великобритания, Меморандум № 5736/G, 1939 год. Долгосрочный план действий по противодействию СССР;

• США, закон № 402, 1948 год, который заставлял СМИ «оказывать планомерное и систематическое воздействие на общественное мнение других народов»;

• США, директива № 68, 15 апреля 1950. Директива ставила задачу «обеспечить коренное изменение природы советской системы, посеять внутри этой системы семена ее разрушения, поощрять и поддерживать беспорядки и мятежи в избранных, стратегически важно расположенных странах — соседях СССР».

В хрущёвские и брежневские времена американская агитация успешно сдерживалась железным занавесом и цензурой. Относительно малочисленные диссиденты были вполне безобидны, значительная их часть работала на КГБ.

В горбачёвский период однако взятый на «гласность» и «перестройку» курс открыл американцам дорогу к беззащитным мозгам советских людей. Потребовалось всего несколько лет, чтобы в СССР начались настоящие революционные брожения.

Их итогом стал распад Советского Союза и фактическое подчинение властей новообразованной России добрым американским советникам.

В дикие девяностые годы западная точка зрения на Россию стала общепринятой и практически официальной. Федеральные телеканалы чуть ли не прямым текстом называли Россию позорной страной несчастных недолюдей, которая должна стыдиться самого факта своего существования.

Поворот к лучшему произошёл в первой половине нулевых годов, когда сменивший Ельцина Владимир Путин «равноудалил» самых одиозных олигархов и забрал у них часть властных рычагов. Официальные телеканалы нехотя, но начали выражать хотя бы формально пророссийскую точку зрения на текущие события. Тем не менее, радиостанции, газеты и, конечно же, Рунет сохранили почти безусловную лояльность Западу.

В 2011 году, после решения Путина участвовать в президентских выборах 2012 года, информационное давление на Россию резко усилилось. Было создано коллаборационистское движение «Белая Лента», организованы стотысячные прозападные митинги в Москве. В Рунете развернулась полномасштабная травля российских властей, которая даже отодвинула на второй план традиционную травлю собственно России и русских.

В качестве обратной реакции на успехи западной пропаганды внутри России начали набирать силу пророссийские сообщества и СМИ. На внешних же фронтах России удалось организовать успешную контратаку при помощи стратегического наступательного телеканала Russia Today, ставшего самым популярным новостным каналом на YouTube и самым востребованным зарубежным телеканалом не только в странах Запада, но и во многих странах, в которых Запад ранее единолично контролировал информационное поле.

В начале 2014 года трагические события на Украине серьёзно дискредитировали либеральные идеи, а убедительная победа России на Олимпиаде в Сочи сильно подняла престиж нашей страны: прежде всего, в глазах самих россиян. Возвращение Крыма в Россию стало поворотной точкой: это событие вызвало настоящий взрыв патриотизма внутри России — который, впервые за 25 лет постсоветской истории — был в полном объёме поддержан федеральными телеканалами.

Россияне начали не только массово интересоваться политикой, но и оценивать политическую ситуацию со строго пророссийских позиций.

Дальнейшие события 2014 года — начало гражданской войны на Донбассе, введение санкций против России, взятие Соединёнными Штатами ответственности за обрушение курса рубля — только ослабили позиции западной пропаганды и пробудили в русских казалось бы давно забытое чувство упрямой решимости сражаться до победного конца. Готова ли Россия противостоять информационной атаке исходящей от развитых стран? Ответ на этот вопрос лучше всего дать, проанализировав некоторые события недавнего прошлого. 2008 г. - год «информационного прессинга». Одним из основных и самых печальных событий 2008 г. стала война между Южной Осетией и Грузией.

Опыт современных локальных конфликтов учит, что любая «обычная» война должна предваряться мощной информационной войной. Чтобы убедиться в этом, приведём несколько примеров. События в Южной Осетии комментировали многие западные СМИ. Так, британский телеканал «Sky News» показал в новостном выпуске 8 августа видеосюжет об обстреле сёл Южной Осетии и столицы республики — Цхинвала грузинской артиллерией в ночь на 8 августа, а на следующий день сопроводил его сообщением, что «Россия ведёт обстрел территории Южной Осетии, входящей в состав Грузии».

Долгое время западные телевизионные каналы не вели репортажи непосредственно из Цхинвала, однако почти все сообщали о катастрофических разрушениях города сначала под огнём грузинской артиллерии, затем под огнём артиллерии российской. Все представители западных СМИ базировались в Тбилиси и сообщали о разрушениях в грузинских городах Гори и Поти. В Цхинвале находились только российские телеканалы и один украинский. И только впоследствии Цхинвал посетили более 100 иностранных журналистов.

Российский информационный канал «Вести» приводит слова депутата Европарламента Джульетто Кьеза, что итальянские СМИ «сообщают о том, что Грузия была подвергнута атаке со стороны Южной Осетии, что Россия ведёт войну против Грузии с целью захвата этой страны. Это сплошная ложь»3. Фиксировались и другие факты фальсификации со стороны итальянского телевидения.

14 августа председатель комитета Госдумы по международным делам Константин Косачёв заявил, что западные СМИ, в частности американский телеканал CNN, «безобразно» освещали события в Южной Осетии: «почти сутки CNN, BBC и другие каналы не показывали и сейчас не показывают Цхинвали». По его словам, в определённый момент на CNN и BBC до буквы совпал даже заголовок новостей — «Грузия сражается». И на фоне этого — картинки разрушенных домов — неважно, кем они разрушались, неважно, что это грузины стреляли по Цхинвалу, добавил Косачёв. «Всё это очень удобно ложится в ту теорию, которую до сих пор исповедовал Запад по отношению к „свободной демократической Грузии“ и по отношению к „агрессивной России“, которая эту Грузию пытается как-то подавить», — заявил Косачёв.

12 августа бывший президент СССР Михаил Горбачёв заявил, что после нападения грузинской стороны на Цхинвал обвинения в адрес России в «агрессии „против маленькой беззащитной Грузии“ выглядят не только лицемерными, но и бесчеловечными». По мнению Горбачёва, в западной прессе не получили должного освещения последствия гуманитарной катастрофы. 15 августа Горбачёв оправдал помощь России Южной Осетии, заявив: «Россия действовала, отвечая на агрессию с грузинской стороны. Нельзя было оставить без внимания такой разгром и уничтожение людей». Горбачёв вновь отметил однобокость и предвзятость западных СМИ в освещении событий, выразив по этому поводу своё сожаление.

21 августа правозащитник, директор Московского бюро по правам человека Александр Брод отметил необъективность зарубежных СМИ и правозащитных

организаций в освещении событий. «Вчера был весьма показательный звонок из Риги. Звонили из русской газеты люди, которые прочли на информационных лентах о нашей встрече в Общественной палате. Для них было просто открытием, насколько страшной была бойня в Южной Осетии. Видимо, своё представление о произошедшем коллеги формировали на основе материалов CNN и зарубежных информагентств, где Россия абсолютно неоправданно рисовалась агрессором». По его мнению, некоторые правозащитные организации стремятся умолчать о погибших жителях Южной Осетии или занизить цифры. Как сказал Брод, «зарубежные коллеги либо не удосужились приехать в республику, либо высасывали информацию из пальца»4.

26 августа российский телеведущий Владимир Познер, комментируя в эфире радиостанции «Эхо Москвы» освещение событий в Южной Осетии западным телеканалами, заявил: «Ощущения мерзостные. Мерзостные по всем азимутам. Но самые мерзостные, мне трудно говорить, но самые мерзостные американские, конечно. . Просто полное вранье. Там вообще не говорилось о том, что что-то было в Цхинвали. То есть у рядового американца такое впечатление, что Россия вторглась в Грузию. Почему вторглась, вот потому что русские такие. Россия такая. Путинская Россия. Медведев это с их точки зрения, опять как он подаётся, это прилежный ученик Путина. Насчёт того, что такое Южная Осетия, что такое Абхазия, ну ни малейшего, ноль. То есть, и мне так это было обидно, потому что я помню, какое было американское телевидение, какие там были люди. Как это всё подавалось. Сейчас это просто какой-то ужас»5.

27 августа профессор Барселонского университета Франсиско Вейга заявил, что в испанской прессе были опубликованы многочисленные смонтированные фотографии грузин — жертв конфликта. По его словам, «одновременно на страницы испанских СМИ не попала ни одна фотография жертв среди населения столицы Южной Осетии Цхинвали, вызванных варварскими бомбардировками грузинской армии»6.

8 сентября журналисты телеканала Russia Today обвинили CNN в подлоге и грубой фальсификации. По их словам, американский телеканал, демонстрируя кадры разрушений осетинского Цхинвала, заявил, что речь идёт о грузинском Гори. Один из журналистов сказал по поводу освещения событий западными СМИ: «Война Грузии в Южной Осетии нанесла катастрофический удар по их репутации. Впервые они замалчивали события в военном конфликте, а порой, как показал пример с CNN, занимались и фальсификацией»1. Подобные сообщения появлялись и ранее.

Приведённые выше факты — это лишь небольшое свидетельство того, что Россия противостояла в информационной войне фактически всему миру. Хотя российскую военную кампанию на Северном Кавказе можно считать победной, но Россия, на мой взгляд, однозначно проиграла информационную войну, которую против нас развернули США. В глазах практически всех государств мира Россия выглядит агрессором, напавшим на слабую Грузию.

В чём причина информационного поражения? В нежелании руководства России создавать за рубежом мощную информационную службу, способную противостоять информационным атакам? Кто-то утверждает, что это не так, у нас есть информационные службы, которые регулярно и своевременно распространяли информациюо грузино-югоосетинском конфликте, но мировые СМИ не брали её или коверкали, исполняя политический заказ. Безусловно, большинство крупных западных СМИ жёстко ангажированы и заточены под определённую политическую пропаганду, однако в свое время в СССР СМИ были куда более подконтрольными и цензурированными, но это не мешало США проводить пропаганду своих ценностей на территории Союза. Это не помешало укрепить в сознании жителей СССР мнение, что западный образ жизни много лучше советского.

На мой взгляд, вопрос лишь в профессионализме информационных служб. Просто в США есть профессионалы, которые гораздо лучше наших могут работать со СМИ и умеют распространять нужную им информацию. Наши информационные службы полностью теряются, если нет возможности подкупать журналистов, покупать СМИ целиком или отдать приказ «сверху» на размещение нужного материала. И это при том, что всё это — нормальные действия в сложных политических ситуациях. Однако сейчас ситуация хуже, чем кажется. Поэтому России в ближайшее время нужно сформулировать и дать адекватный информационный ответ, в первую очередь — на европейском и постсоветском пространстве. Прошедшее после «пятидневной августовской войны» на Кавказе время показало, что пока российская политическая элита пытается сделать соответствующие выводы после информационной агрессии США, Великобритании и ряда других стран против России. Прошло несколько публичных мероприятий с участием ведущих российских экспертов, на которых анализировался ход информационной войны против России (17 сентября 2008 г. Общественной палатой организован круглый стол «Информационная агрессия против России: методы противостояния», 2 октября 2008 г. партией «Справедливая Россия» проведена международная конференция «Информационные войны в современном мире»).

Главная проблема, которая была очевидной в ходе дискуссий, — это явная недооценка роли информационного противоборства современной российской политической элитой в условиях усиления глобальной экономической и геополитической конкуренции в мире. После принуждения Грузии и её заокеанских покровителей к миру геополитическая и геоэ-кономическая роль России в мире во многом будет определяться тем, сможет ли она создать эффективную систему информационного противоборства. Время требует одновременного создания мощных информационно-аналитических и информационно-пропагандистских структур, предназначенных для реализации информационных моделей урегулирования конфликтов.

Если вернуться к вопросу, готова ли Россия противостоять информационному прессингу, то на основе вышеизложенных фактов напрашивается однозначный ответ, что без умения управлять информационными процессами современное государство

так же бессильно, как не имеющее армию. В каком-то смысле информационная служба так же важна и необходима, как армия.

Главные направления антироссийской пропаганды:

• Разжигание розни: в первую очередь межнациональной и межрелигиозной; разжигание ненависти к евреям, к выходцам с Кавказа и республик Средней Азии, к православным, к мусульманам, к иудеям и так далее.

• Организация и поддержка сепаратистских настроений. Упор тут делается на Кавказ и Татарстан, однако последние годы активизировалась работа американцев в Сибири и на Дальнем Востоке.

• Разжигание ненависти к представителям власти: в первую очередь к полиции и к чиновникам.

• Точечная травля президента России и главных его сподвижников.

• Продвижение проектов «Такая-то страна не Россия». Самый известный проект — «Украина не Россия», однако аналогичные проекты поддерживаются Вашингтоном во всех республиках СССР.

• Реклама направленной на дезинтеграцию России идеи «Хватит кормить таких-то»: «Хватит кормить Кавказ», «Хватит кормить хохлов», «Хватит кормить Москву»

• Пропаганда разного рода чернухи: в первую очередь экономической, социальной. На базе чернухи продвигается идея «мы движемся к пропасти, надо срочно свергать власть».

• Продвижение русофобских идей, согласно которым русские — ущербный народ, который не имеет права ни на патриотизм, ни на собственное государство.

• Реклама достижений Запада: как реальных, так и вымышленных, направленная в том числе на пропаганду эмиграции из России на Запад.

• Прямая пропаганда идей «майдана» — свержения власти под предлогом борьбы с «коррупцией» и «тиранией».

• Создание в странах Запада образа агрессивной и вероломной России, с которой нельзя иметь никаких дел.

• Создание в республиках СССР образа нищей и отсталой России, которая во всём уступает Западу.

В настоящее время Россия оказывает успешное сопротивление атакам США: прежде всего за счёт хорошей работы телевидения и за счёт проигрышной для Запада тактики прямого давления на Россию.

Несмотря на превосходство противника в численности и мастерстве, ситуация складывается в целом в пользу России.

Государство хоть и медленно, но призывает к порядку принадлежащие ему СМИ. Тот факт, что против России ведётся информационная война, был, наконец, признан официально и открыто — с 26 декабря 2014 года в военной доктрине России в качестве одной из внутренних и внешних угроз названо информационное воздействие на население с целью подрыва исторических, духовных и патриотических традиций в области защиты Отечества, а также разжигание межнациональной и межрелигиозной розни.

Всё больше появляется пророссийских блогеров и общественных деятелей. У многих людей наступает передозировка русофобии: им надоедают потоки грязи, которые льются изо всех щелей на их страну. Наконец, люди становятся опытнее: после краткого периода слепой эйфории они начинают видеть нестыковки и передёргивания во вражеской агитации.

Становится всё сложнее отрицать тот факт, что против России ведётся настоящая информационная война — особенно после того, как Штаты открыто заявляют о запуске новых проектов по ведению информационной войны против России. Люди со здоровой моралью не допускают возможности принимать участие в информационной войне на стороне врагов России.

Наконец, мы находимся на своей территории, а наш противник вынужден орудовать на чужой: он плохо понимает наши реалии, и регулярно допускает из-за этого болезненные просчёты.

С 2007 по 2015 год число россиян, не доверяющих иностранным СМИ, увеличилось в 7 раз — до 50 %.

Можно уже констатировать факт: в 2014 году в информационной войне произошёл перелом в нашу пользу. Однако пока наши успехи ограничиваются преимущественно внутренним фронтом. На Западе СМИ продолжают с помощью привычных методов пропаганды и разнообразных провокаций выстраивать негативный образ России. Однако и там есть успехи: работа телеканала RT, международного информагентства Sputnik и прочих иноязычных российских СМИ впервые в истории дала западному обывателю возможность систематически знакомиться с российским взглядом на важнейшие мировые события.

Заключение. «Информационная война» — термин, безусловно, важный и актуальный на современном этапе развития общества, без четко понимания которого нельзя понять процессы, происходящие в современной политической жизни и геополитике.

В настоящее время понятие «информационная война» определяется по-разному. Это связано с многозначностью термина «information warfare», что породило множество разночтений при его переводах. Он может трактоваться как «информационная война», «информационное противоборство», «информационно-психологическая война». В частности, информационная война характеризуется как информационная деятельность, предпринимаемая политическим образованием (например государством) для ослабления, уничтожения другого политического образования; как информационная борьба между соревнующимися конкурентами; информационный военный конфликт между двумя массовыми врагами, например армиями и т. п.

Мировое информационное пространство в XXI веке заполнено информационными войнами. С каждым годом их количество растет и уже термин «информационная война» воспринимается без удивления и становится обычным явлением во время как внутригосударственного, так и международных конфликтов.

Многие предполагают, что информационные войны пришли к нам только в XX веке, вместе с эрой технологий, но это не так.

Россия в настоящее время также становится участником информационных войн, и вынуждена разрабатывать оборонительные мер для защиты населения страны.

МОЛОДЕЖНЫЙ ЭКСТРЕМИЗМ В СОЦИАЛЬНЫХ СЕТЯХ (Кузеванова О.О.)

Введение. С развитием технологий, в первую очередь в сети Интернет, существенно расширяются возможности личности для разнообразных видов деятельности. Население России, особенно молодое, охвачено Интернетом и социальными сетями. Возможности общения пользователей отличают социальные сети от других Интернет-ресурсов: характерной чертой социальных сетей является высокий уровень интерактивности, при котором скорость обмена информацией и скорость общения зачастую не уступают общению вне сети.

В настоящее время различные социальные институты, явления и процессы обретают новые, ранее неизвестные формы. Это относится в полной мере и к такому негативному социальному явлению, как экстремизм, проявляющемуся в политической, экономической, социальной, религиозной и других сферах общественной жизни. Рост влияния глобальной сети Интернет оказал значительное влияние на экстремизм, значительно обострив данную социальную проблему, особенно в молодежной среде.

Современное общество является совокупностью людей, исповедующих самые различные ценности, обладающих передовыми способами получения информации и связи друг с другом, способных навязывать свою волю большинству с помощью различных технологий. Все эти факторы свидетельствуют о значительной сложности, которая стоит перед органами власти по профилактике и недопущению роста экстремистских настроений и мероприятий, проведенных на этой основе.

Вопрос об уровне толерантности российского общества является сегодня критически важным. Этим обусловлена необходимость формирования толерантных отношений у молодёжи. Обострение межнациональных конфликтов, усиление тенденций проявления ксенофобии –проблемы современной России. Сложная социально-экономическая обстановка, геополитические изменения и значительные миграционные потоки непосредственно влияют на общественное мнение в области межэтнических отношений.

Экстремизм в молодежной среде – один из самых опасных и сложно прогнозируемых феноменов современности, способный распространять свое влияние на различные сферы общественной жизни. Экстремизм превратился в весомый фактор дестабилизации социально-экономической и политической ситуации в мире. Неудивительно, что специфика его проявлений привлекает внимание представителей различных социогуманитарных наук, которые подчеркивают системный и многоаспектный характер этого явления.

Таким образом, можно сделать вывод, что *в условиях развитых Интернет-коммуникаций заявленная тема в среде молодежи весьма актуальна.*

Общая характеристика экстремизма в молодежной среде. В ст. 1 ФЗ N 114-ФЗ «О противодействии экстремистской деятельности» (далее – ФЗ N 114-ФЗ)[148], закреплено понятие экстремизм. Оно громоздко, но того требует практическая деятельность. Опираясь на ст. 1 ФЗ N 114-ФЗ, экстремизм можно **определить** как деятельность организаций либо физических лиц, направленная на насильственное изменение основ конституционного строя и нарушение целостности РФ; публичное оправдание терроризма и иная террористическая деятельность; возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; воспрепятствование осуществлению гражданами их избирательных прав и др.

В психологической и юридической литературе экстремизм рассматривается как приверженность крайним взглядам и мерам. Так, Р. М. Узденов предлагает определить экстремизм как «социальное, негативное явление, проявляющееся в совокупности общественно опасных уголовно наказуемых деяний, совершаемых в соответствии с определенной системой взглядов, воззрений, убеждений, возведенных в культ, с целью достижения определенного результата, предусмотренного этой системой взглядов, в какой-либо области общественных отношений, существующий порядок в которой отрицается экстремистами»[149].

Однако считаем данное определение слишком абстрактным. Для правоприменителя необходима конкретика, то есть определенный перечень деяний, которые можно считать экстремисткой деятельностью. Поэтому считаем определение в ст. 1 ФЗ N 114-ФЗ соответствующим запросам практической деятельности.

Согласно **социологическому опросу**[150], проведенному в г. Москва среди 2400 жителей, терроризм является наиболее опасной формой экстремизма в оценках горожан. Такого мнения придерживается 52,7% участников исследования. Экстремизм и терроризм соотносятся как общее и частное: первый образует своеобразную идеологическую основу террористическим действиям; второй - определяется совокупностью крайних установок (обоснованием применения насилия) для достижения политических целей нелегитимным способом.

На втором месте по уровню социальной опасности экстремистских проявлений москвичи назвали межнациональные конфликты. По мнению 25,1% горожан межэтнические конфликты представляют угрозу для безопасности города, следовательно, необходимо осуществлять комплекс мероприятий, направленных на снижение агрессии в отношениях людей, разных национальностей. Особенно это актуально в том контексте, что столица имеет печальный опыт массовых социальных

[148] Федеральный закон от 25.07.2002 N 114-ФЗ (ред. от 23.11.2015) "О противодействии экстремистской деятельности"// Собрание законодательства РФ, 29.07.2002, № 30, ст. 3031

[149] Узденов, Р. М. Экстремизм: криминологические и уголовно-правовые проблемы противодействия : автореф. дис. ... канд. юрид. наук. М., 2008. 29 с.

[150] См. Приложение №1.

выступлений, поводом к которым служили преступления, совершенные представителями этнических меньшинств.

Среди преступлений против основ конституционного строя и безопасности государства экстремизм является одним из самых опасных преступных деяний, посягающим не только на основы конституционного строя и безопасность государства, о чем свидетельствует ряд факторов. Во-первых, экстремистская деятельность осуществляется в основном в соучастии. Причем распространенными формами соучастия в данных деяниях выступают особые организованные формы преступной деятельности: экстремистское сообщество и экстремистская организация. Во-вторых, такие преступления, как терроризм, бандитизм, захват заложника, массовые беспорядки, хулиганство, вандализм и иные, при определенных условиях являются преступлениями экстремистского характера, а также во многих случаях выступают в качестве способа реализации экстремистской деятельности. [151]

Наибольшие опасения вызывает экстремистское поведение молодежи, так как отмечается, что **экстремизм во всем мире «молодеет»**: в большей степени совершают преступления молодые люди в возрасте 15-25 лет.[152]. По замечаниям исследователей, «экстремальность молодежи может приобретать крайние, главным образом спонтанные черты, которые нередко перерастают в экстремистские настроения[153]».

Отметим, что наблюдается рост числа молодёжных объединений экстремистской направленности. Всё чаще в экстремистскую деятельность втягивается студенчество. Так, только в 2009 году в России проведено свыше 27 тыс. общественно-политических акций, вызванных осложнением социально-экономической ситуации российских регионов, в которых приняло участие более 5 млн. 380 тыс. человек. В ходе массовых акций зарегистрировано свыше 2 тыс. правонарушений[154].

По данным МВД России, за последние пять лет количество преступлений экстремистской направленности возросло более чем в четыре раза. Так, в 2009 году на территории Российской Федерации зарегистрировано 548 таких преступлений, что на 19,1% больше аналогичных показателей 2008 года. При этом только за первые месяцы 2010 года совершено около 600 преступлений, основное участие в совершении которых приняли молодые люди в возрасте от 14 до 30 лет[155].

---

[151] Алехин Е.В. Совершенствование законодательства как направление противодействия деятельности экстремистских сообществ // Российский следователь. 2011. № 3. С. 26.

[152] Терешина Е. А. Противодействие молодежному экстремизму (на примере опыта Великобритании и США) // КПЖ. 2015. №1. URL: http://cyberleninka.ru/article/n/protivodeystvie-molodezhnomu-ekstremizmu-na-primere-opyta-velikobritanii-i-ssha (дата обращения: 10.12.2016).

[153] Зинурова Р. И., Тузиков А. Р. Тренды молодежной политики за рубежом // Вестник Казанского технологического университета. 2012. Т. 15. № 10. С. 345-348.

[154] Абалов И.Ю. Об использовании неформальными молодёжными объединениями сети интернет в целях осуществления экстремистской деятельности// Практические аспекты профилактики экстремизма и противодействия распространению его идеологии в молодежной среде : сборник научных трудов международной заочной научно-практической конференции. – Орехово-Зуево : Изд-во МГОГИ, 2013. – 172 с.

[155] Статистика Департамента по противодействию экстремизму МВД России // Коммерсант ВЛАСТЬ № 13 (917) от 4 апреля 2011. С. 31.

Особенность молодежных экстремистских групп заключается в следующем: низкий уровень образования (школа, максимум - колледж); низкий уровень культуры (уровень интересов ограничен сферой массовой культуры); цели сосредоточены на достижении материальных благ, бездуховность, отсутствие морально-нравственных ценностей, нарушение родительско-детских отношений, сформированное в результате невозможности достижения желаемых целей, реализации своего потенциала, ощущение ненужности, ущербности; приверженность установкам, оправдывающим и даже возвеличивающим агрессивные алгоритмы поведения (фильмы, передачи, сериалы, статьи, компьютерные игры)[156].

По идейно-политической направленности молодёжные экстремистские объединения можно подразделить следующим образом:

– леворадикальные (радикальные коммунисты, анархисты, анархо-коммунисты и так далее);

– либерально-демократические;

– праворадикальные (национал-патриоты, националисты, неофашисты, неонацисты);

– религиозные (приверженцы деструктивных религиозных культов);

Наибольшую опасность представляют молодёжные объединения **праворадикальной идейно-политической направленности**, деятельность которых отличается особой жестокостью, высоким уровнем организации и многочисленностью, наличием достаточно развитой идеологической составляющей, активным использованием разнообразных агитационно-пропагандистских форм и методов.

Проблема агрессивного и экстремистского поведения молодежи становится все более актуальной в условиях российской действительности. Элементы экстремистского поведения молодежи формируются на фоне деформации социальной и культурной жизни общества. В **перечень основных причин роста экстремистского поведения молодежи** исследователи склонны включать следующее: социальное неравенство, желание самоутвердиться в мире взрослых, недостаточную социальную зрелость, неконтролируемые процессы миграции, а также недостаточный профессиональный и жизненный опыт, а следовательно, и сравнительно невысокий (неопределенный, маргинальный) социальный статус[157].

Абалов И.Ю. отмечает ряд факторов, определяющих специфику развития экстремизма в молодёжной среде:

– долговременность, разнообразие, латентность и комплексный характер причин и условий, обусловливающих возникновение и распространение экстремизма в целом;

---

[156] Васенина И. Ценностные ориентации студенческой молодежи и экстремизм // Высшее образование в России. 2007. № 11. - С. 116—119.

[157] Бааль Н.Б. Политический экстремизм молодежи как острейшая проблема современной России // Российский следователь. 2007. № 7. С. 27. Т

– наличие достаточно развитой идеологической составляющей, в том числе в форме экстремистской идеологии, концепций, доктрин и программ экстремистской деятельности, играющих возрастающую роль в её осуществлении;

– возрастающую роль в экстремистской деятельности молодёжных объединений агитационно-пропагандистских форм и методов её осуществления, все более активно используемых для пропаганды идеологии и практики экстремистской деятельности и её оправдания;

– усиление влияния религиозного и этнонационального фактора в развязывании и развитии конфликтов, возникающих в молодёжной среде;

– тенденциозное использование экстремистски настроенной молодёжью существующих в различных социальных слоях населения – с разной степенью остроты и распространённости – предубеждений, заблуждений и фобий[158].

Кубякин Е.О. считает, что **возникновение и развитие молодежного экстремизма обусловлено рядом объективных и субъективных факторов,** связанных как с особенностями духовного, личностного облика молодежи, так и с социальными, экономическими, культурными условиями ее существования в 1990–2000-х гг[159]:

К числу **объективных факторов** генезиса молодежного экстремизма можно отнести:

– системные, не решаемые годами проблемы российского общества в виде коррупции, кризиса правоохранительной системы, теневой экономики, резкого расслоения общества на «богатых» и «бедных» и т. д.;

– падение духовно-нравственного уровня населения России вследствие «засилья» образцов массовой культуры, культа наживы, успеха, физической силы, гедонизма, «легких денег»;

– дисбаланс системы социализации, воспитания, социального развития молодого поколения;

– дисфункциональность системы средств массовой коммуникации, ее отказ от обсуждения множества социальных проблем с одновременным усилением пропаганды ксенофобии в отношении, в частности, выходцев из регионов Северного Кавказа и Средней Азии;

– негативные последствия войны в Чечне и миграционной политики;

– социокоммуникативные изменения и становление глобального информационного общества, бурное развитие инновационных СМК, в первую

158

Абалов И.Ю. Об использовании неформальными молодёжными объединениями сети интернет в целях осуществления экстремистской деятельности // Практические аспекты профилактики экстремизма и противодействия распространению его идеологии в молодежной среде : сборник научных трудов международной заочной научно-практической конференции. – Орехово-Зуево : Изд-во МГОГИ, 2013. – 172 с.

159 Кубякин Евгений Олегович Тенденции развития молодежного экстремизма в условиях прогресса информационно-компьютерных технологий // Вестник МГИМО. 2013. №3 (30). URL: http://cyberleninka.ru/article/n/tendentsii-razvitiya-molodezhnogo-ekstremizma-v-usloviyah-progressa-informatsionno-kompyuternyh-tehnologiy (дата обращения: 10.12.2016).

очередь Интернета, что привело к практически полной потере контроля государства над процессом коммуникации с молодым поколением.

К **числу субъективных факторов генезиса** молодежного экстремизма, непосредственно связанных с социально-возрастными, социально-психологическими и социокультурными характеристиками молодежи, можно отнести:

– экстремальность как имманентное свойство сознания и поведения молодежи, в ряде случаев способное трансформироваться в экстремизм;

– не сформировавшееся до конца сознание, социокультурный облик, в результате чего молодой человек рискует попасть под влияние идеологов экстремизма;

– маргинальный, неустойчивый переходный социальный статус молодежи (во многих случаях отсутствие семьи, детей, престижной работы и т.п.) приводит ее к мысли о том, что «нечего терять»;

– эмоционально-чувственное, аффективное восприятие окружающей действительности;

– жажда новизны, поиск способов самореализации, к сожалению, участие в экстремистской деятельности в ряде случаев удовлетворяют данные потребности молодежи;

– некритическое, парадоксальное мышление и отсутствие жизненного опыта, неумение анализировать причины и последствия социальных действий и взаимодействий.

Каким бы комплексом факторов не был обусловлен экстремальный тип сознания молодежи (психофизиологическим, социокультурным, социально-статусным), очевидно, что он выступает «фактором риска» в молодежной среде в аспекте потенциального генезиса экстремизма.

Экстремизм в социальных сетях. Технически, **социальная сеть является объединением группы людей на одной Интернет-платформе**, позволяющей пользователю загружать свой контент и обмениваться им с другими пользователями. Интернет-пользователи объединяются в социальную сеть на базе специального Интернет-ресурса. Интерфейс социальной сети предусматривает регистрацию участника, предоставляет участнику возможность наполнять ресурс своим контентом в свободном режиме, вести блоги, которые также свободно могут комментироваться другими участниками социальной сети. Большая часть социальных сетей располагают инструментами чатов, где участники могут общаться в реальном времени.

Интернет становится мощным инструментом молодёжных объединений экстремистской направленности. Этому способствует специфика глобальной сети, которая предоставляет такие преимущества как простота доступа, независимость от географического расположения, неограниченная потенциальная аудитория, трудность контроля со стороны правоохранительных органов и другие. Членам экстремистских объединений уже не нужно лично встречаться для обмена информацией,

согласования планов и координации преступных действий[160]. Если еще 10-15 лет назад деятельность экстремистских движений, групп локализовывалась пространственными границами города, района, области, то сейчас, благодаря информационно-коммуникационным технологиям, и, прежде всего, Интернету, экстремистская деятельность становится элементом медийной повестки дня в масштабах страны, а то и всего русскоязычного сегмента СМК (в частности, Рунета)[161].

Еще несколько лет назад Сеть представляла собой огромное виртуальное хранилище информации, что-то вроде гигантской постоянно обновляемой энциклопедии. Пока Интернет был медленный и дорогой, в нем, также, как и в бумажных книгах и газетах из рук в руки, существовала четкая граница между автором и читателем. В сегодняшнем Интернете преобладают так называемые (проекты web 2.0, есть usergenerated content, содержание, создаваемое пользователями). [162]

Особенности распространения информации в социальных сетях определяют их значение, которое трудно переоценить. Информация может распространяться как новостная рассылка от сообщества, в котором состоит пользователь социальной сети, так и непосредственно от пользователя к пользователю, что и обуславливает **скорость ее распространения.** Естественно, что данный медийный инструмент имеет свою специфику и может быть использован для публикации материалов экстремистской направленности[163].

Так, например, показательно дело, рассмотренное Индустриальным районным судом г. Барнаула Алтайского края[164]. Рассмотрев в судебном заседании уголовное дело в отношении Т., обвиняемого в совершении преступлений, предусмотренных ч.1 ст.282 УК РФ, ст. 319 УК РФ, суд установил : Т. совершил действия, направленные на возбуждение ненависти, вражды, а также на унижение достоинства человека, группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, совершенные публично.

---

[160] Абалов И.Ю. Об использовании неформальными молодёжными объединениями сети интернет в целях осуществления экстремистской деятельности // Практические аспекты профилактики экстремизма и противодействия распространению его идеологии в молодежной среде : сборник научных трудов международной заочной научно-практической конференции. – Орехово-Зуево : Изд-во МГОГИ, 2013. – 172 с.

[161] Кубякин Е.О. Молодежный экстремизм в сети интернет как социальная проблема // Историческая и социально-образовательная мысль. 2011. № 4 (9)

[162] Алпатова Д., Левкина Е., Высоцкий А., Диденко Р. Экстремизм в социальных сетях: причины, условия, противодействие // Экстремизм в молодежной среде : причины, условия, профилактика. Сборник материалов научных работ преподавателей и студентов юридического факультета и факультета массовых коммуникаций, филологии и политологии АлтГУ. / Отв.ред. В.А.Мазуров, В.В.Русанов - Барнаул: Алтайский госуниверситет, 2015. – С. 64. (289 с.

[163] Гладышев-Лядов Владимир Социальные сети как инструмент для пропаганды экстремизма // Обзор. НЦПТИ. 2013. №2. URL: http://cyberleninka.ru/article/n/sotsialnye-seti-kak-instrument-dlya-propagandy-ekstremizma (дата обращения: 14.12.2016).

[164] URL: http://industrialny.alt.sudrf.ru/modules.php?id=130&name=docum_sud

Кроме того, Т. совершил публичное оскорбление представителя власти в связи с исполнением им своих должностных обязанностей**.** Преступления совершены Т. при следующих обстоятельствах. В период времени с 15 часов 28 минут *** сентября 2006 г. по *** ноября 2006 г., более точно время не установлено, Т., находясь в квартире по адресу: г. Барнаул, ул. ***, **используя персональный компьютер, имеющий DSL – подключение к сети Интернет с абонентского №***, умышленно с целью возбуждения национальной и религиозной вражды, унижения** национального достоинства, пропаганды исключительности, превосходства русскоязычного населения Российской Федерации над другими народами **по их национальному призна**ку и отношению к религии, **действуя публично, с использованием сети Интернет**, обращаясь к **неограниченному числу пользователей сетью Интернет**, а именно, создав FTP-каталог ***, доступный для просмотра неограниченному числу пользователей сети Интернет, в открытой и доступной для понимания форме, посягая на честь и достоинство граждан, их конституционные права и свободы, в нарушение п. 2 ст. 19 Конституции РФ, гарантирующей равенство прав и свобод человека и гражданина независимо от расы, национальности и отношения к религии, п. 2 ст. 29 Конституции РФ, запрещающей пропаганду социального, национального, религиозного и языкового превосходства, являясь приверженцем национал-патриотических и националистических взглядов, используя сеть Интернет, **разместил на FTP-каталоге *** сети Интернет, тексты и сюжеты, являющиеся средством разжигания национальной, расовой, религиозной ненависти и вражды и возбуждающие национальную, религиозную вражду.**

Так, в видео-текстовых и графических файлах, размещенных Т. на FTP-каталоге *** сети Интернет, содержатся унизительные характеристики, отрицательные эмоциональные оценки и негативные установки в отношении лиц.

Тексты и сюжеты, размещенные на FTP-каталоге *** сети Интернет, содержат резкую негативную оценку этнических групп и групп лиц, объединенных по расовому признаку, и выражают неприязненные, враждебные отношения к указанным группам.

Таким образом, обвиняемый Т. путем вышеуказанных действий в наглядной демонстративной форме формировал и подкреплял негативный стереотип евреев, китайцев, цыган, лиц кавказской национальности, жителей Средней Азии, этнических групп и групп лиц, объединенных по расовому признаку по отношению к русской нации.

Вина Т. подтверждается следующими доказательствами по делу: Свидетель Г**.** показал в судебном заседании, что осенью 2006 г., проводя проверку на FTP-каталогах местных провайдеров, он обнаружил папку ***. В ней были расположены видеоролики насильственного характера в отношении лиц нерусской национальности, а также две фотографии, на одной из которых было изображено лицо, похожее на Президента РФ Путина В. В. в одежде скинхэда с надписью «Мочи чурок». Об обнаружении указанных материалов были составлены соответствующие документы.

Согласно заключению комиссионной политолого-лингвистической экспертизы, значением изображения лица, похожего на Президента РФ, а также сопровождающей данное изображение надписи, является призыв к насильственным действиям против коренных жителей Кавказа, Закавказья и Средней Азии. **Приговором от 20 августа 2008 г. Индустриального районного суда г. Барнаула признан виновным Т. в совершении преступления, предусмотренного ч.1 ст. 282 УК РФ.**

Пропаганда политического экстремизма также имеет свою специфику. Помимо информационной функции социальные сети могут выполнять и **функции по организации и координации массовых акций**, имеющих своей целью открытую конфронтацию законно избранной власти. В виртуальном пространстве осуществляется управление деятельностью автономных групп, идеологическая работа, сбор средств, а также непосредственная подготовка к совершению экстремистских акций.

Одной из главных задач, решаемых молодёжными экстремистскими объединениями с помощью Интернета, является как можно более **широкое освещение экстремистских акций** с привязкой их к идеологическим посылам экстремистов и устрашением общества. Прекращение деятельности таких Интернет-ресурсов зачастую невозможно в силу правовых и юридических сложностей, а иногда малоэффективно, так как их место быстро занимают новые.

Кроме того, Интернет используется для привлечения и «мобилизации» сторонников, играющих важную роль в поддержке экстремистских объединений. Следует отметить активное использование таких социальных сетей, как «Одноклассники.ru», «Вконтакте» и других для анализа личной информации, вводимой пользователем при регистрации на сайте или в опросах, по которой можно определить его отношение к той или иной проблеме.

В настоящее время социальные сети зачастую действуют в **симбиозе с традиционными СМИ**, играя роль распределителя готового контента. Помимо распределительной функции, социальные сети зачастую исполняют роль информагентства, предоставляя СМИ информацию, на основании которой и создается готовый новостной и аналитический контент. В качестве примера можно отметить частое появление роликов с видеохостинга Youtube.com в новостных и аналитических передачах центральных телеканалов.

Если новостное Интернет-издание публикует материал экстремистской направленности, то у государства есть эффективные рычаги воздействия в виде УК РФ и единого списка экстремистских материалов, посредством которых можно достаточно оперативно ограничить доступ Интернет-пользователей к вышеуказанным материалам, а в некоторых случаях даже ограничить доступ к самому сайту, на котором они опубликованы. Социальные сети контролировать гораздо сложнее, нежели обыкновенные Интернет-сайты. Российская **социальная сеть «Вконтакте», по заявлениям ее пресс-службы, активно сотрудничает с органами внутренних дел в плане удаления экстремистских материалов**, но, несмотря на это, сеть

изобилует группами, которыми ведется открытая пропаганда религиозного экстремизма и фундаментализма, группами, размещающими материалы, которые можно причислить к политическому экстремизму.

Зарубежные социальные сети находятся вне поля российского законодательства, потому фактически они являются открытой площадкой для публикации материалов экстремистской направленности. Однако следует отметить, что и российская аудитория этих сетей гораздо меньше аудитории у российских социальных сетей и пропаганда в них не особо эффективна в отношении наших сограждан[165].

Используя социальные сети, члены экстремистских движений, групп получили возможность вступать в дискуссии, спорить, отстаивать свою идеологию, убеждения в Интернет-ресурсах, где численность аудитории может колебаться от нескольких десятков до сотен тысяч человек. Под видом «обмена мнениями» в Интернете экстремисты получили возможность вести пропаганду, вербовать новых сторонников и увеличивать количество «сочувствующих». Эта проблема в настоящее время недооценивается в России. Ситуация осложняется тем, что молодое сознание до конца не сформировано, опытные экстремисты могут использовать сложившуюся ситуацию в целях насаждения выгодных им установок. Молодежь нуждается в повышенном внимании со стороны общественности, государственных управленческих структур, так как в силу своих социально-психологических и социально-возрастных особенностей может подвергаться влиянию экстремистских движений, групп[166].

Психически неустойчивой личности не нужно слишком много времени, чтобы изменить свои гуманистические взгляды если не сразу на взгляды экстремистские, то приближенные к таковым. Молодой человек без крепкого внутреннего стержня легко поддается влиянию экстремистских идей, ведь их, во-первых, достаточно много в количественном выражении, чем идей толерантных,

а во-вторых, образ их подачи более выраженный и агрессивный[167].

Число лиц, приговоренных к реальным срокам заключения за нарушение антиэкстремистского законодательства в интернете, растет, говорится в докладе центра «Сова» по итогам 2014–2015 гг[168]. В 2015 г. по сравнению с предыдущим годом этот показатель вырос с 18 до 43 человек. В большинстве случаев осужденные высказывались против власти и президента, против вооруженного вмешательства России в дела Украины или призывали к вооруженному джихаду. Кроме того, за два года к обязательным работам приговорены 106 человек, к штрафам – 64, к

[165] Гладышев-Лядов Владимир Социальные сети как инструмент для пропаганды экстремизма // Обзор.НЦПТИ. 2013. №2. URL: http://cyberleninka.ru/article/n/sotsialnye-seti-kak-instrument-dlya-propagandy-ekstremizma (дата обращения: 14.12.2016).

[166] Кубякин Евгений Олегович Молодежный экстремизм в сети Интернет как социальная проблема // ИСОМ. 2011. №4. URL: http://cyberleninka.ru/article/n/molodezhnyy-ekstremizm-v-seti-internet-kak-sotsialnaya-problema (дата обращения: 14.12.2016).

[167] Котлярова В.В., Шубина М.М., Сысоева О.Н. Молодежный экстремизм в социальных сетях: специфика и теоретическое осмысление // URL: https://almavest.ru/ru/archive/1866/3469

[168] См. Приложение № 2

исправительным работам – 59. Основной объем криминального преследования интернет-пропаганды приходится на этноксенофобов, второе место занимают радикальные исламисты. Большинство дел было возбуждено за размещение информации в сети «В контакте» – 207 дел за два года, в Facebook – всего два уголовных дела. При этом число осужденных за посты выросло за год в 2 раза. В 2015 г. за ненадлежащую фильтрацию «экстремистского» контента были оштрафованы как минимум 17 физических и юридических лиц, было вынесено 14 предупреждений интернет-СМИ. В 2015 г. из 232 приговоров за публичные высказывания, отнесенные к экстремистским, 194 приговора были вынесены за интернет-высказывания[169].

Зачастую такие дела получают резонансный характер. Так, например, было с привлечением к ответственности за снимок со свастикой произошло с Полиной Петрусевой, журналистом смоленского портала readovka.ru. В январе 2015 года девушка выложила на странице в соцсети "ВКонтакте" фотографию своего дома времён нацисткой оккупации. В частности, правоохранителей не устроило изображение флага Третьего рейха, которое было видно на документальном снимке. В конечном счёте Петрусеву оштрафовали на тысячу рублей за пропаганду и публичное демонстрирование нацистской символики[170]. Однако Роскомнадзором утверждено, что изображения свастики без целей пропаганды допустимы, поэтому данная ситуация и получила противоречивый характер.

Для молодежи особенно важно сохранить баланс между мерами безопасности, принятыми на уровне государства, и существующими гражданскими правами. Хотя необходимо признать, что в условиях социальной нестабильности зачастую сложно сделать выбор: либо в пользу авторитета безопасности страны и ее граждан, либо в пользу авторитета свободы.

Проведенный 2-5 июля 2010 Аналитический Центр Юрия Левады (Левада-Центр)[171] социологический опрос по репрезентативной выборке 1600 россиян в возрасте 18 лет и старше в 130 населенных пунктах 45 регионов страны показал, что в России растет количество граждан, которые не считают возможным приравнивать к экстремизму публичные высказывания, неприемлемые для большинства, если в них не содержится призывов к насилию. Их число увеличилось с 36% в июле 2002 до 53 в июле 2010. Противоположного мнения сегодня придерживаются 23%респондентов (в июле 2002 – 35%). Еще четверть россиян затрудняются с ответом. При этом 39% россиян опасаются, что в ближайшее время власти могут начать преследование любой критики в свой адрес под предлогом профилактики экстремизма в России. 31% респондентов отвечают, что это скорее невозможно. Еще 30% затруднились ответить. Эти ожидания остаются стабильными с конца 2006 года (год первого замера).

[169] URL: http://www.vedomosti.ru/politics/articles/2016/06/29/647196-sazhayut-ekstremistskie-viskazivaniya

[170] URL: https://life.ru/t/технологии/421282/statia_za_pieriepost_za_kakiie_vyskazyvaniia_v_sotssietiakh_mozhno_siest

[171] См. Приложение 3

Острота и масштабность, многообразие форм проявлений экстремизма в молодёжной среде определяют важность организации эффективного нейтрализующего воздействия на весь комплекс связанных с ним угроз и формирующих его негативных факторов социальной среды. С учётом повышенной общественной опасности и роста количества экстремистских проявлений, особенно в молодёжной среде, противодействие этому явлению должно стать одним из приоритетных направлений работы уполномоченных государственных органов (субъектов противодействия экстремизму). При этом особое значение имеет пресечение попыток использования молодёжными объединениями экстремистской направленности возможностей сети Интернет и электронных средств массовой информации для осуществления психологического воздействия на массовое сознание, а также для пропаганды экстремизма и терроризма[172].

Согласно проведенному нами опросу, в котором участвовали студенты-юристы (112 человек), состоящие в группе «Юридический факультет АлтГУ» в социальной сети «Вконтакте», **41,4% (46 человек)** опрошенных считают, что суду при назначении наказания за экстремистские интернет-высказывания необходимо учитывать количество подписчиков того блога (группы, страницы человека в социальной сети), на котором размещена данная информация, так как это влияет на степень общественной опасности, а **58,6% (65 человека)** опрошенных считают, что это не необходимо, так как независимо от количества подписчиков, данное высказывание может повлиять на конкретного человека и подтолкнуть его к совершению экстремистских действий[173].

Социологические исследования показывают, что решить проблему экстремизма в молодежной среде можно следующими методами: снижением уровня безработицы (особенно среди молодежи); активизацией работы силовых ведомств по борьбе с экстремизмом; ограничением пропаганды агрессии и насилия в СМИ[174]; совершенствованием нормативно-правовой базы в данной сфере;; повышением доступа к получению молодежью высшего, средне-специального, профессионального образования, внедрением здорового образа жизни; усилением роли воспитания в духе традиций национальной культуры; предоставлением молодежи больших возможностей для участия в решении социальных, политических и экономических и других проблем страны и региона[175].

Для эффективной **борьбы с пропагандой экстремизма** в социальных сетях необходимо использование высокотехнологичных, передовых компьютерных программ для осуществления постоянного онлайн-мониторинга. Без таких программ

---

[172] Абалов И.Ю. Об использовании неформальными молодёжными объединениями сети интернет в целях осуществления экстремистской деятельности// Практические аспекты профилактики экстремизма и противодействия распространению его идеологии в молодежной среде : сборник научных трудов международной заочной научно-практической конференции. – Орехово-Зуево : Изд-во МГОГИ, 2013. – 172 с.

[173] См.Приложение № 4

[174] Берковец Л. Агрессия: причины, последствия, контроль. – М.: Олма-пресс, 2001.

[175] Смирнов В. А. Основы молодежной политики в сфере профилактики экстремизма // Вестник ЧГУ. Серия Философия. Социология. Культурология. 2008. № 14. Вып. 7. - С. 78-87.

борьба с интернет-экстремистами напоминает печально известную борьбу с «ветряными мельницами». Скорость обработки и анализа существующих интернет-ресурсов существенно меньше, чем скорость появления новых или закрытия ранее существовавших. Кроме того, «традиционный» контент-анализ вступает в противоречие с такой электронной коммуникационной структурой, как Интернет. Объем и скорость распространения информации в Интернете никак не соответствует возможностям традиционного контент-анализа. Именно поэтому можно утверждать, что в настоящее время назрела необходимость активного внедрения программного обеспечения для проведения компьютерного контент-анализа интернет-ресурсов. «Ручной» мониторинг сети не успевает за развитием событий в ней. Экстремисты, имея значительный ресурс времени, спокойно совершают свои противоправные деяния и уходят от ответственности. Один закрытый сайт сменяет другой, аналогичной направленности. Компьютерная программа должна в режиме реального времени выявлять акты экстремизма и позволять оперативно реагировать на это силовым структурам. Необходимо корректировать и антиэкстремистское законодательство. Только комплексными мероприятиями можно решить проблему интернет-экстремизма[176].

Терешина Е.А. отмечает: Противостоять экстремизму и различным молодежным экстремистским группам можно и нужно на комплексной основе. Весь комплекс содержит условно **три механизма воздействия** на экстремистские и ксенофобские настроения молодежи в современном обществе:

- нормативно-правовые и организационные рычаги регулирования (законы и государство);

- институты гражданского общества (семья, система образования);

- средства массовой информации (СМИ), сети Интернет.[177]

Одним из немаловажных элементов противодействия является **профилактика экстремизма**. Это комплекс мероприятий, включающий воспитательную работу с молодёжью, организацию соответствующего информационного сопровождения деятельности органов государственной власти в средствах массовой информации, использование положительного потенциала общественных и религиозных объединений. Поддерживаемые органами власти различного уровня молодёжные проекты, студенческие движения способны выступить альтернативой деструктивной деятельности объединений экстремистской направленности. **Укрепление патриотизма и гражданской ответственности** в молодежной среде, уважение к другим национальностям, чужой культуре, открытость и толерантность – одно из действенных средств борьбы с экстремизмом, но только при условии объединения усилий всех государственных и общественных структур. Необходимо приложить

[176] Кубякин Евгений Олегович Молодежный экстремизм в сети Интернет как социальная проблема // ИСОМ. 2011. №4. URL: http://cyberleninka.ru/article/n/molodezhnyy-ekstremizm-v-seti-internet-kak-sotsialnaya-problema (дата обращения: 14.12.2016)

[177] Терешина Е. А. Противодействие молодежному экстремизму (на примере опыта Великобритании и США) // КПЖ. 2015. №1. URL: http://cyberleninka.ru/article/n/protivodeystvie-molodezhnomu-ekstremizmu-na-primere-opyta-velikobritanii-i-ssha (дата обращения: 10.12.2016).

максимальные усилия, чтобы показать молодежи, что есть другие возможности для высказывания своего мнения и самореализации, нежели уход от законности и мирного существования.

Современный опыт многих западноевропейских стран и США свидетельствует об относительно успешной деятельности государственных и гражданских структур в области профилактики молодежного экстремизма. В контексте правового противодействия экстремизму в Великобритании в 2007 г. была принята **программа «Предупреждение насильственного экстремизма»** (Preventing Violent Extremism)[178]. Эта стратегическая программа направлена на пресечение всех попыток распространения экстремистских идей. Она основана на принципе «четырех «П»: предупреждение, преследование, протекция и подготовка. В дальнейшем на основании этого документа МВД представило в парламент Великобритании перечень мер по борьбе с экстремизмом. В частности, ведомство предложило **закрыть въезд в страну иностранцам, замеченным или подозреваемым в экстремизме** или пропаганде незаконных или общественно опасных действий. Этот закон запретил въезд в страну неонацистов и иных экстремистов. **В 2006 г. в целях борьбы с молодежным экстремизмом правительство Великобритании издало специальную директиву по борьбе с пропагандой и распространением экстремизма в университетах и колледжах страны**[179]. Противодействие экстремизму на организационном уровне в Великобритании осуществляют МВД, Кабинет министров, полиция.

По мнению **Г.К. Нурлыбаевой**, борьба с молодежным экстремизмом часто ведется «точечно», в эту борьбу вовлекаются небольшие полицейские подразделения графств, отдельных городов и поселений. Полиция обращает внимание на тех, кто ведет подпольную подрывную и агитационную работу в общинах, выявляет случаи подготовки к экстремистской деятельности, анализирует улики, о которых сообщает население [180].

По мнению специалистов, по сравнению с другими странами Европы, «уровень молодежного экстремизма в Великобритании достаточно низок». Примечательно, что страна имеет свои особенности. Здесь наблюдается национальное, религиозное и этническое разнообразие.

В Великобритании противодействие экстремизму осуществляется также на общегражданском уровне. Так, во всех общеобразовательных учреждениях Великобритании в учебные планы введен обязательный предмет «Гражданское образование». Без целенаправленного формирования национального и гражданского

[178] Preventing Violent Extremism URL: https://www.gov.uk/government/organisations/homeoffice (дата обращения: 08.12.2016).

[179] Малышев В.В. Европейский опыт противодействия экстремизму // Правовая инициатива/ 2013. № 8. С. 2.
[180] Нурлыбаева Г.К. Молодежный экстремизм и особенности противодействия со стороны полицейских служб Великобритании // Российский следователь. 2011. № 10. С. 34.

самосознания у подростков и молодежи невозможно выстроить эффективную систему профилактики экстремизма и др. негативных явлений в обществе[181].

В США противодействие экстремизму (в том числе и терроризму) рассматривается как одно из приоритетных направлений политики в области обеспечения национальной безопасности. Необходимо отметить, что понятие экстремизма в США не употребляется. В свою очередь наказание предусматривается за деяния, получившие обобщенное название «hate speech» (речи ненависти) или «hatred crime» (преступления ненависти). Речь идет прежде всего о возбуждении национальной, расовой и религиозной вражды, об оскорблениях, угрозах и насилии в отношении лиц по причине их принадлежности к какой-либо общности, о распространении литературы и идеологии расистского и иной направленности. В законодательстве западных стран применяются такие понятия, как «дискриминация», «ксенофобия», «антисемитизм», «исламофобия», «разжигание национальной или религиозной вражды». Уголовные законы штатов США дают правовое определение преступлениям на почве ненависти и ужесточают наказание за них. В средствах массовой информации США к экстремистам относят как террористов, так и всех лиц, которые пропагандируют насилие на почве расовой, политической, национальной и религиозной ненависти[182].

На борьбу с экстремизмом в США направлены усилия, практически, всех звеньев государственного аппарата. Основная ответственность возложена на Министерство внутренней безопасности. В его рамках существует Совет внутренней безопасности, который является механизмом координации усилий исполнительных органов власти США, вырабатывающих и реализующих политику безопасности внутри страны[183].

В целях борьбы с молодежным экстремизмом **в США создан Национальный центр предупреждения преступлений, совершаемых молодежными группировками экстремистской направленности по мотивам расово-этнической ненависти**. Основными направлениями деятельности Центра выступают:

- сбор информации о преступлениях, совершаемых по мотивам расово-этнической ненависти и преступниках, совершающих такие преступления;
- подготовка на основе полученной информации статей, брошюр о борьбе с преступлениями, совершаемых по мотивам расово-этнической ненависти.

В деятельность по пресечению экстремизма **в США активно вовлекаются структуры гражданского общества – общественные организации (аналитические центры),** а также образовательные учреждения. Аналитические центры (Институт

[181] Терешина Е. А. Противодействие молодежному экстремизму (на примере опыта Великобритании и США) // КПЖ. 2015. №1. URL: http://cyberleninka.ru/article/n/protivodeystvie-molodezhnomu-ekstremizmu-na-primere-opyta-velikobritanii-i-ssha (дата обращения: 10.12.2016).

[182] Система мер по противодействию терроризму в США. Сайт Национального Центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет (НЦПТИ). URL: http://ncpti.ru/articles/?ELEMENT_ID=178 (дата обращения: 11.12.2016).

[183] National Security Council website. URL: http://www.whitehouse.gov/administration/eop/nsc (дата обращения: 11.12.2016).

мира, Антидиффамационная лига, Южный центр по защите гражданских прав, **Международный центр развития толерантного сознания** и предотвращения экстремизма) занимаются переработкой информации об активности экстремистов, готовят рекомендации в сфере противодействия экстремизму и терроризму, вырабатывают тактические практические решения для органов государственной власти США. **При университетах** Америки и во многих мечетях также действуют центры, реализующие программы толерантности, снижения рисков формирования групп радикально настроенных мусульман. **При каждом полицейском управлении** существует своя общественная палата из представителей этнических общин и религиозных лидеров. Представители правозащитных организаций зачастую на общественных началах являются советниками начальника полиции в том или ином городе. В школах и университетах США преподаются учебные дисциплины, способствующие формированию гражданского самосознания и антитеррористического мировоззрения молодого поколения, в числе которых «Граждановедение» (школа), «Международная безопасность» и «Глобальный терроризм» (в Колумбийском, Вашингтонском и Стэнфордском университетах).

Немаловажным механизмом противодействия экстремизму среди молодежи являются СМИ и глобальная сеть Интернет. Молодые люди все чаще проводят время у мониторов своих компьютеров. Причем информация, которая заполняет Интернет- пространство, не подвергается отбору со стороны самих молодых людей, что в свою очередь не является безопасным. **Во всех развитых западных странах функционирует практика блокирования экстремистских сайтов**. Комитет ООН по правам человека в общих замечаниях № 34, касающихся ст. 19 Международного пакта об общественных и политических правах, отметил, что ограничение функционирования сайтов и блогов является абсолютно правомерным, если они экстремистские.

В декларации Комитета министров Совета Европы о правах человека и о правовом государстве (CM (2005)56) указывается, что национальные правительства должны вести борьбу с экстремистским контентом в Интернете, носящим, например, расистский характер. США в области противодействия экстремистским сайтам преуспело. Согласно отчету Google, американское правительство пытается контролировать потоки информации в Интернете гораздо чаще, чем правительство любой другой страны в мире. За прошедший 2013 г. в США было подано более 2000 запросов на удаление виртуальных личных страниц [184].

Необходимо отметить, что правовая сфера российского Интернета приближена к стандартам западных стран. В России с 2014 г. вступила в силу поправка к закону «Об информации, информационных технологиях ии о защите информации», которая **допускает оперативную досудебную блокировку Интернет-сайтов с экстремистским контентом.** Эти законы не являются посягательством на свободу

[184] Как законы Евросоюза и США борются с неофашизмом, экстремизмом, подрывной деятельностью и клеветой. URL: http://www.whitehouse.gov/administration/eop/nsc (дата обращения: 10.12.2016).

слова граждан страны, наоборот, в сети Интернет закроются возможности для пропаганды экстремизма, терроризма и ксенофобии.

Заключение. Проведенный анализ зарубежного опыта в области противодействия молодежному экстремизму свидетельствует о том, что эффективность работы в данной области зависит от ряда факторов:

- наличие политической воли руководителей, заинтересованных в выработке эффективной молодежной политики отдельных стран и всего мирового сообщества;
- четкая нормативно-правовая база (разграничение и конкретизация на теоретико-методологическом уровне определений «экстремизм», «ксенофобия», «расизм»);
- надлежащая квалификация кадров, создание дополнительных ответственных структур, четкая согласованность действий и скоординированные усилия сторон;
- участие в различных образовательных программах и проектах в области профилактики экстремизма самой молодежи.

Формы и способы борьбы с экстремизмом и терроризмом необходимо развивать и совершенствовать. Международное сообщество не должно довольствоваться наработанными методами и средствами противодействия данным социальным проявлениям. Важным является продолжение работы в сфере совершенствования законодательства и направлений международного противодействия экстремизму и терроризму на современном этапе по следующим направлениям:

1. Заключение международных договоров о создании общеевропейской системы сбора данных об авиапассажирах, призванной повысить эффективность борьбы с международным терроризмом и организованной преступностью.
2. Создание единой нормативно-правовой базы, направленной на расширение сотрудничества следственных и судебных органов.
3. Разработка законопроектов об обязательном установлении административного надзора за гражданами, которые были осуждены за совершение экстремистских и террористических преступлений и освободились из мест заключения.
4. Своевременное включение в списки зарубежных террористических организаций различных радикальных сект и групп.
5. Совершенствование профессиональной и организационно-управленческой подготовки кадров, задействованных на контртеррористическом направлении, включая парламентариев, сотрудников правоохранительных органов, судебной и пенитенциарной систем, криминалистов, юристов, адвокатов и т.д.

Необходимо констатировать, что России необходимо наличие эффективных структур (программ), которые будут осуществлять мониторинг интернет-пространства (в том числе, социальных сетей) и немедленно сообщать правоохранительным органам о факте распространения экстремистских материалов.

Приложение № 1

Объем выборки респондентов - 2400 человек из числа жителей города Москва. Терроризм является наиболее опасной формой экстремизма в оценках горожан.[185]

Приложение № 2

Приложение № 3

[185] АНАЛИТИЧЕСКИЙ ОТЧЕТ по результатам социологического исследования Жители Москвы о путях борьбы с экстремизмом, терроризмом и прочими девиациями// http://dsmir.mos.ru/napravleniya_deyatelnosti/sotsiologicheskie_issledovaniya/oprosy_obshchestvennogo_mneniya_v_2014_godu/Extremism.pdf

Можно ли считать экстремизмом публичное высказывание каких-либо взглядов, неприемлемых для большинства, если в этих высказываниях не содержится призывов к насилию**?**

	июл.02	июл.07	июл.10
определенно да	12	11	3
скорее да	23	23	20
скорее нет	29	31	42
определенно нет	7	8	11
затруднились ответить	30	29	25

Чаще других отвечают, что призыв к насилию не обязательное условие для определения экстремистских высказываний, респонденты 25-54 лет, с низким и средним потребительским статусом. Не согласны с ними чаще россияне18-24 лет, с высоким уровнем дохода.

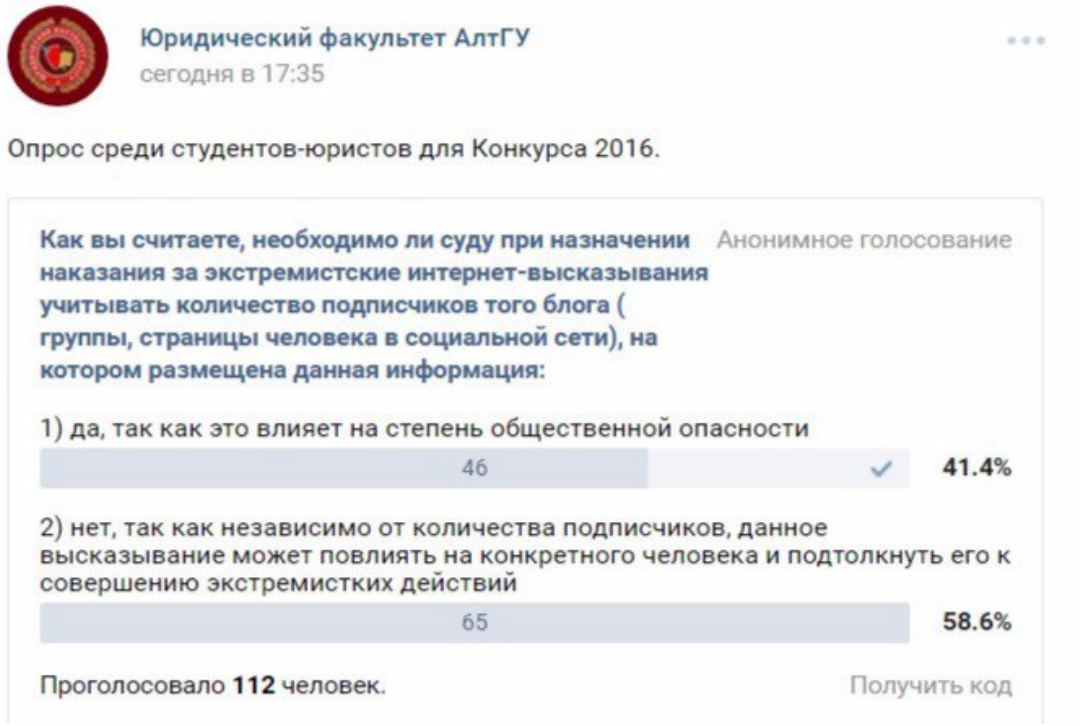
Возможно ли, что под видом борьбы с экстремизмом в России в ближайшее время будет запрещена любая критика власти?

	дек.06	июл.07	июл.10
определенно да	9	8	8
скорее да	30	28	31
скорее нет	27	28	28
определенно нет	8	6	3
затруднились ответить	26	31	30

В той или иной степени, ожидают таких действий от власти чаще мужчины, респонденты 40-54 лет, с высшим образованием. Считают, что это скорее невозможно, россияне 18-39 лет также лица с высшим образованием и высоким потребительским статусом.[186]

Приложение № 4

[186] ***Борьба с экстремизмом и критика власти в России***
// http://www.levada.ru/2010/07/26/borba-s-ekstremizmom-i-kritika-vlasti-v-rossii/


Юридический факультет АлтГУ
сегодня в 17:35
Опрос среди студентов-юристов для Конкурса 2016.
Как вы считаете, необходимо ли суду при назначении наказания за экстремистские интернет-высказывания учитывать количество подписчиков того блога (группы, страницы человека в социальной сети), на котором размещена данная информация:
Анонимное голосование
1) да, так как это влияет на степень общественной опасности
46
41.4%
2) нет, так как независимо от количества подписчиков, данное высказывание может повлиять на конкретного человека и подтолкнуть его к совершению экстремистких действий
65
58.6%
Проголосовало 112 человек.
Получить код

НЕКОТОРЫЕ ПРОБЛЕМЫ УСТАНОВЛЕНИЯ ПРИЗНАКОВ СОСТАВА ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТКОЙ НАПРАВЛЕННОСТИ В СОЦИАЛЬНЫХ СЕТЯХ (Данилова Р.Р.).

Введение. XXI век называют веком информационного общества, основой которого, несомненно, являются информационные и коммуникационные технологии, получившие широкое применение[187]. Сеть «Интернет» расширяет и упрощает возможности общения людей, распространения и поиска информации. В то же время достижения научно-технического прогресса активно используются в целях распространения противоправной информации, нарушающей права физических и юридических лиц, интересы и безопасность общества и государства[188].

Актуальность работы обусловлена тем, что в настоящее время активно задействуются новые технологии для совершения прежних преступлений. Это порождает совершенствование способов совершения последних, а, следовательно, и определенные трудности в доказывании совершенных деяний.

Объектом исследования являются преступления экстремисткой направленности совершенные в сети «Интернет», а именно ч. 2 ст. 280, ч. 2 ст. 280.1 и ч. 1 ст. 282 Уголовного кодекса Российской Федерации (далее – УК РФ)[189].

Целью написанной работы является обозначение проблем, с которыми сталкиваются органы предварительного следствия и суды, при расследовании дел экстремисткой направленности совершенных на просторах сети «Интернет».

Для достижения поставленной цели необходимо решить следующие задачи: определить степень опасности новых способов распространения материалов экстремистской направленности, проанализировать судебную практику и действующее законодательство в обозначенной сфере, выяснить, как в зарубежных странах разрешаются проблемы, которые имеются в России.

Методологией исследования явились современные методы познания, метод теоретического анализа: изучение, анализ, синтез и обобщение научной и учебной литературы, анализ нормативно-правовых актов и судебной практики, а также метод системного анализа. Применение этих методов позволило проанализировать и выявить поставленные мною задачи.

Структура работы состоит из титульного листа, введения, трёх глав, заключение и список используемой литературы.

Распространение информации экстремисткой направленности в социальных сетях как угроза национальной безопасности. Один из признаков

[187] Власова, Н.В., Грачева, С.А., Мещерякова М.А. Правовое пространство и человек: монография / Н.В. Власова, С.А. Грачева, М.А. Мещерякова [Электронный ресурс] // Сайт портала информационно-правового обеспечения Гарант. URL: http://base.garant.ru/57736904/#ixzz4SjGJzL35 (дата обращения 10.12.2016)
[188] Там же.
[189] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 22.11.2016) // Собрание законодательства РФ. – 1996. – №25. – Ст. 2954

государства, как известно, является его суверенитет. Конституция Российской Федерации (далее – РФ) провозглашает наше государство таковым (ст. 4)[190]. Постановлением Конституционного Суда РФ от 07.06.2000 N 10-П установлено, что суверенитет представляет собой необходимый качественный признак Российской Федерации как государства, означающий верховенство, независимость и самостоятельность государственной власти, полноту законодательной, исполнительной и судебной власти государства на его территории и независимость в международном общении[191].

Президентом РФ 28 ноября 2014 года утверждена «Стратегия противодействия экстремизму в РФ до 2025 года»[192]. Ее цель – защита основ конституционного строя РФ, общественной безопасности, прав и свобод граждан от экстремистских угроз. Для эффективного достижения поставленной цели предлагается реализация Стратегии в три последовательных этапа и с 2016 года начался второй из них. Одно из мероприятий обозначенном на данном этапе является создание системы дополнительной защиты информационно-телекоммуникационных сетей, включая сеть «Интернет», от проникновения экстремистской идеологии.

12 мая 2009 года Президентом РФ подписан Указ «О Стратегии национальной безопасности Российской Федерации до 2020 года»[193]. В данном документе определены основные понятия, например, что такое «национальная безопасность» – это состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие России, оборону и безопасность государства[194]. Не маловажным является определение «угрозы национальной безопасности», под которой понимается прямая или косвенная возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию РФ, обороне и безопасности государства[195].

Далее п. 10 выделяет в качестве негативного влияния на национальные интересы силовые подходы в международных отношениях, противоречия между основными участниками мировой политики, а также совершенствование форм противоправной

---

[190] Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 (ред. от 21.07.2014) // Российская газета. – 1993. – 25 декабря

[191] По делу о проверке конституционности отдельных положений Конституции Республики Алтай и Федерального закона «Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации»: постановление Конституционного Суда РФ от 07.06.2000 N 10-П // Российская газета. – 2000. – 21 июня (№118).

[192] Стратегия противодействия экстремизму в Российской Федерации до 2025 года. Консультант Плюс: Справочно-правовая система [Электронный ресурс] / ЗАО «Консультант Плюс». – Версия 2016. – Заглавие с экрана. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=194160;fld=134;dst=1000000001,0;rnd=0.8380356376128439 (дата обращения 05.12.2016)

[193] О Стратегии национальной безопасности Российской Федерации до 2020 года: указ Президента Российской Федерации от 12 мая 2009 г. N 537// Российская газета. – 2009. – 19 мая (№4912)

[194] Там же.

[195] О Стратегии национальной безопасности Российской Федерации до 2020 года: указ Президента Российской Федерации от 12 мая 2009 г. N 537// Российская газета. – 2009. – 19 мая (№4912)

деятельности в кибернетической и биологической областях, в сфере высоких технологий. П. 37 одним из источников угроз России указывает экстремистскую деятельность националистических, религиозных, этнических и иных организаций и структур, направленная на нарушение единства и территориальной целостности, дестабилизацию внутриполитической и социальной ситуации в стране.

Данные положения приведены неслучайно, они напоминают, не так давно произошедшие, события, так называемой, «арабской весны». Именно в этом историческом событии впервые социальные сети сыграли значительную роль в организации массовых общественных беспорядков в странах Азии, Африки и Ближнего Востока. Популяризация крупных международных (Twitter, MySpace, Facebook, YouTube) и внутригосударственных социальных сетей вызывает интерес и обеспокоенность со стороны большинства современных государств и органов, компетентных в сфере безопасности[196]. Примером являются ограничения на использование социальных сетей, вводимые в Соединенных Штатах Америки.

В последние годы публичные призывы к осуществлению экстремистской деятельности при помощи сети «Интернет» стали одним из наиболее популярных видов преступлений экстремисткой направленности[197]. Статистика показывает, что, если в 2007 г. из 28 приговоров по ст. 280 и 282 УК только 3 приговора касались размещенных в сети материалов, то в 2008 г. – 14 из 45, в 2009 г. – 17 из 56, в 2010 г. – 26 из 72, а в 2011 г. – 52 из 78[198] (см. Приложение 1). А только за первые полгода 2016 г. к ответственности за экстремизм были привлечены 398 человек[199]. Вместе с тем увеличивается Федеральный список экстремистских материалов. По состоянию на 9 апреля 2016 года в нем находилось 3364 Интернет-ресурса, а по состоянию на 9 декабря 2016 года – 3991[200] (см. Приложение 1). Таким образом, за 8 месяцев их число увеличилось на 627 сайта.

Число пользователей социальными сетями с каждым годом только увеличивается, что говорит о потребности в урегулировании отношений в данной области. К январю 2015 года население России составляло 146,3 млн. людей,

---

[196] Власова, Н.В., Грачева, С.А., Мещерякова М.А. Правовое пространство и человек: монография / Н.В. Власова, С.А. Грачева, М.А. Мещерякова [Электронный ресурс] // Сайт портала информационно-правового обеспечения Гарант. URL: http://base.garant.ru/57736904/#ixzz4SjGJzL35 (дата обращения 10.12.2016)

[197] Михеев, А.В. Особенности доказывания публичных призывов к осуществлению экстремистской деятельности в сети Интернет/А.В.Михеев// Консультант Плюс: Справочно-правовая система [Электронный ресурс] / ЗАО «Консультант Плюс». – Версия 2015. – Заглавие с экрана. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=CJI;n=80197 (дата обращения 08.12.2016)

[198] Троегубов Ю.Н. Проблемы противодействия экстремизму в сети Интернет [Электронный ресурс] Научная электронная библиотека «Киберленинка». – Заглавие с экрана. URL: http://cyberleninka.ru/article/n/problemy-protivodeystviya-ekstremizmu-v-seti-internet (дата обращения 08.12.2016)

[199] Лайк не преступление [Электронный ресурс] Интернет-портал «Российской газеты». – Режим доступа: https://rg.ru/2016/11/03/verhovnyj-sud-rekomendoval-ne-nakazyvat-za-reposty-v-socialnyh-setiah.html (дата обращения 13.12.2016)

[200] Федеральный список экстремистских материалов [Электронный ресурс]. – Сайт Министерства юстиции РФ. – Заглавие с экрана. URL: http://minjust.ru/extremist-materials?field_extremist_content_value=&page=16 (дата обращения 09.04.2016 и 09.12.2016)

количество интернет-пользователей – 87,5 млн., а количество активных аккаунтов в соц. сетях – 67,0 млн., что на 10% больше чем в 2014 году[201].

Значительную угрозу представляет экстремистская деятельность националистических, религиозных, этнических и иных организаций и структур, направленная на нарушение единства и территориальной целостности государства, дестабилизацию внутриполитической и социальной ситуации в стране. Их идеи пропагандируются в Интернете посредством функционирования сайтов и иных ресурсов, на которых размещается информация экстремистского характера. Экстремистские, как и террористические организации, находят своих сподвижников в социальных сетях, в которых представлена в отрытом доступе необходимая информация о человеке.

Другим источником угрозы государственной и общественной безопасности является разведывательная и иная деятельность специальных служб и организаций иностранных государств, а также отдельных лиц, направленная на нанесение ущерба безопасности Российской Федерации[202]. Так, социальные сети могут быть использованы для вербовки агентов иностранными разведками, сбора информации о сотрудниках конкурентных спецслужб, выяснения общественного мнения и отношения пользователей к последствиям планируемых операций, а также для оказания корректирующего воздействия на общественное сознание, дестабилизацию обстановки в странах-противниках и т.д.[203].

Как видим, Интернет-пространство нуждается в надежной системе безопасности, как и любая социально значимая инфраструктура. Система безопасности должна строиться на единых принципах и системе мер, обеспечиваемых всеми ее участниками. При этом особое внимание необходимо уделить обеспечению безопасного использования социальных сетей.

Проблемы установления признаков составов преступлений экстремисткой направленности. Прежде всего, следует обозначить особенности совершения преступления в сети Интернет. Традиционно к ним относят латентность, поскольку весьма сложно отследить действия каждого интернет-пользователя. Кроме того, даже при наличии материала он должен будет подвергнут оценки специалиста, на первый взгляд бывает очень трудно сказать относятся ли те или иные сведения к экстремистским.

Другой спецификой данных преступлений является распространенность субъектов в пространстве. Нет каких-либо видимых ограничений для распространения информации по всему миру. Преступник, распространяющий экстремистки контент может находиться в любой точки земного шара, а получателями сообщений может быть неограниченное количество пользователей.

---

[201] Самые популярные социальные сети в России 2015 [Электронный ресурс] Сайт Про СММ. – Режим доступа: http://www.pro-smm.com/populyarnye-socialnye-seti-v-rossii-2015/ (дата обращения 09.12.2016)

[202] О Стратегии национальной безопасности Российской Федерации до 2020 года: указ Президента Российской Федерации от 12 мая 2009 г. N 537// Российская газета. – 2009. – 19 мая (№4912)

[203] Перчаткина, С.А., Черемисинова, М.Е., Цирин, А.М., Цирина, М.А., Цомартова, Ф.В. Социальные интернет-сети: правовые аспекты/С.А. Перчаткина, М.Е. Цирин, А.М. Цирина, Ф.В. Цомартова // Журнал российского права. – 2012. – № 5. – С. 21

Еще одной видимой особенностью преступлений экстремисткой направленности является форма выражения самой информации. Информацию в сети «Интернет» мы воспринимаем лишь зрительно, на каком-либо материальном носители её не существует. В этом, в частности, и заключается опасность такого рода преступления. Удалив или запретив тот или иной материал в одном месте, он легко может возникнуть в другом посредствам создания, например, зеркального сайта[204].

Перечисленные особенности порождают трудности в доказывании составов преступлений экстремисткой направленности совершенных в сети «Интернет».

Одним из ключевых вопросов стоящих перед органами следствия является установление реального, фактического пользователя (IP-адреса) - автора экстремистских высказываний. И здесь возникает две технические проблемы[205]. Первая связана с тем, что беспроводной доступ в сеть (например, Wi-Fi), фактически исключают обнаружение такого лица. Так, летом 2015 года, прокуратура центрального района г. Барнаула оштрафовала местное кафе на 20 тыс. рублей за предоставление доступа в интернет через открытую сеть Wi-Fi[206].

Вторая проблема заключается в сложности идентификации лица как автора или издателя экстремистского материала, а не просто как владельца средства вычислительной техники, посредством которого в сети был размещен материал[207].

В Российской Федерации преступление предусмотренные ч. 2 ст. 280, ч. 2 ст. 280.1 и ч. 1 ст. 282 может совершить физическое, вменяемое лицо, достигшее шестнадцатилетнего возраста, которое разместило информацию экстремисткой направленности в сети Интернет. Таким образом, субъектом указанных преступлений является только автор размещенного текста. О том, как в других странах решен этот вопрос, рассмотрим в гл. 3 настоящей работы.

Так, в 2014 г. по ч. 1 ст. 282 УК РФ был осужден С.Д.Е. публично, разместил в сети «Интернет» на созданной им общедоступной странице социальной текст, начинающийся словами: «Из одной муслимской группы !», и заканчивающейся словами: «Больше чем других христиан! Аллаху Акбар»[208]. В данном материале содержались высказывания, выражающие обоснование необходимости враждебных (насильственных) действий по отношению к группам русских и армян. Что

---

[204] Роскомнадзор начал бороться с "зеркальными" торрентами [Электронный ресурс] Интернет-портал «Российской газеты». – Режим доступа: https://rg.ru/2016/02/29/roskomnadzor-nachal-borotsia-s-zerkalnymi-torrentami.html (дата обращения 13.12.2016)

[205] Троегубов Ю.Н. Проблемы противодействия экстремизму в сети Интернет [Электронный ресурс] Научная электронная библиотека «Киберленинка». – Заглавие с экрана. URL: http://cyberleninka.ru/article/n/problemy-protivodeystviya-ekstremizmu-v-seti-internet (дата обращения 08.12.2016)

[206] Прокуратура Барнаула оштрафовала местную пиццерию за Wi-Fi без пароля «Комитет» [Электронный ресурс] Издательский дом «Комитет». – Режим доступа: https://vc.ru/n/no-free-wifi-in-barnaul (дата обращения 13.12.2016)

[207] Троегубов Ю.Н. Проблемы противодействия экстремизму в сети Интернет [Электронный ресурс] Научная электронная библиотека «Киберленинка». – Заглавие с экрана. URL: http://cyberleninka.ru/article/n/problemy-protivodeystviya-ekstremizmu-v-seti-internet (дата обращения 08.12.2016)

[208] Приговор Индустриального районного суда г. Барнаула Алатйского края от 23 января 2014 г. по уголовному делу №1-54/2014 по обвинению Садовникова Д.Е. в совершении преступления предусмотренного ч.1 ст. 282 УК РФ [Электронный ресурс] // Сайт РосПравосудие. URL: https://rospravosudie.com/court-industrialnyj-rajonnyj-sud-g-barnaula-altajskij-kraj-s/act-459189138/ (дата обращения 13.12.2016)

примечательно, автором данного текста С.Д.Е. не являлся, а размещенный текст скопировал из сети «Интернет», откуда именно следствием не установлено.

Ещё одним вопросом является способ размещения материалов. На характер публичности указано как в ст. ст. 280, 280.1 УК РФ, так и в ст. 282 УК РФ. Интересно в этой связи обратиться к постановлению Пленума Верховного Суда РФ от 28.06.2011 N 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» (далее – ПП ВС №11) в новой редакции от 03 ноября 2016 г[209].

Надо сказать, что до внесения изменений в вышеуказанный акт, практика исходила из виновности лица за «репост» той или иной записи, содержащей материал экстремистской направленности, на свою страницу. Так, к 2 годам лишения свободы условно приговорил Цивильский районный суд Чувашии пенсионера, разместившего у себя на странице (сделал репост записи с иного источника) в соц. сети "ВКонтакте" материал, ранее признанный экстремистским[210]. Также, Московский окружной военный суд оштрафовал студентку, которая перенесла на свою страничку в социальной сети картинку с изображением представителей «ИГ» и «сцены казни», скопировав к видеозаписи текст на русском языке[211].

Теперь п. 8 ПП ВС №11 дополнен абз. 2, в котором сказано: «При решении вопроса о направленности действий лица, разместившего какую-либо информацию либо выразившего свое отношение к ней в сети «Интернет» или иной информационно-телекоммуникационной сети, на возбуждение ненависти либо вражды, а равно унижение достоинства человека либо группы лиц следует исходить из совокупности всех обстоятельств содеянного и учитывать, в частности, контекст, форму и содержание размещенной информации, наличие и содержание комментариев или иного выражения отношения к ней».

Как отметил вице-президент Федеральной палаты адвокатов Генри Резник: «Сам по себе перепост и лайк ни о чем не говорит. Человек может разместить на своей страничке информацию не только потому, что разделяет какое-то мнение. Цель лайка или перепоста может быть даже не в распространении чего-то, а потому что эта статья представляется достаточно интересной сама по себе. Следует допрашивать и выяснять, что было причиной действия. Может быть, он считает, что его друзьям по социальной сети нужно ознакомиться с такой позицией, чтобы в последствие умело противостоять изощренным доводам».

В приведенном выше случае с пенсионером, представляется довольно сомнительным тот факт, что пожилой человек решил разместить у себя на странице подобного рода материал. По словам подсудимого, он не размещал никаких

---

[209] О судебной практике по уголовным делам о преступлениях экстремистской направленности : постановлению Пленума Верховного Суда РФ от 28.06.2011 N 11 (ред. 03.11.2016) // Российская газета. – 2011. – 4 июля (№11).

[210] В Чувашии пенсионера осудили за репост в соцсети [Электронный ресурс] Интернет-портал «Российской газеты». – Режим доступа: https://rg.ru/2016/10/14/reg-pfo/v-chuvashii-pensionera-osudili-za-repost-v-socseti.html (дата обращения 13.12.2016)

[211] Студентку медвуза оштрафовали за перепост экстремистской публикации [Электронный ресурс] Интернет-портал «Российской газеты». – Режим доступа: https://rg.ru/2016/08/18/reg-cfo/studentku-medvuza-oshtrafovali-za-perepost-ekstremistskoj-publikacii.html (дата обращения 13.12.2016)

публикаций на своей странице, а доступ к его аккаунту, в силу небольших познаний им специфики интернета, имеет неограниченное количество людей[212].

Тем не менее, сама сеть «Вконтакте» в Правилах пользования Сайтом, а именно в п. 5.9. устанавливает, что пользователь не имеет права передавать свои логин и пароль третьим лицам и несет полную ответственность за их сохранность, самостоятельно выбирая способ их хранения[213]. В соответствии с п. 5.3.4 данному лицу запрещено загружать, хранить, публиковать, распространять и предоставлять доступ или иным образом использовать любую информацию, которая пропагандирует и/или способствует разжиганию расовой, религиозной, этнической ненависти или вражды, пропагандирует идеологию расового превосходства, а также содержит экстремистские материалы. Сама же администрация сайта с себя всю ответственность за размещенный пользователями контент снимает, о чем говорится в п. 8.2.

Аналогичные правила устанавливают и иные социальные сети, такие как Одноклассники[214], Instagram и др.

На практике встречаются и другие проблемы, их можно выявить, обратившись к судебным решениям. Проанализировав 100 приговоров вынесенных по ч. 1 ст. 282 УК РФ методом случайной выборки с сайта РосПравосудие, можно обратить внимание на следующее. Так, в 31 решении суда не установлено время совершения преступления, в 12 – место совершения преступления, в 4 – сайт с которого была скопирована информация, а в 2 – устройство с которого был размещен материал экстремистского содержания. Общее количество проанализированных дел, имеющие подобные неустановленные факты, составляет 50%.

Опыт зарубежных стран. Изначально отмечу, что правовое регулирование в некоторых зарубежных государствах находится на ином уровне, чем в России. По этой причине некоторые проблемы, которые рассмотрены в гл. 2 настоящей работы, в данных странах не возникают вообще.

Как уже было отмечено, установление субъекта правонарушения связано со значительными трудностями, обусловленными экстерриториальностью Интернета и анонимностью большого числа его пользователей[215]. Во многих зарубежных странах существует определенный подход к решению проблем идентификации пользователей, который заключается в обязательном предоставлении персональной информации при заключении контрактов с интернет-провайдерами на получение услуг доступа в сеть «Интернет».

---

[212] В Чувашии пенсионера осудили за репост в соцсети [Электронный ресурс] Интернет-портал «Российской газеты». – Режим доступа: https://rg.ru/2016/10/14/reg-pfo/v-chuvashii-pensionera-osudili-za-repost-v-socseti.html (дата обращения 13.12.2016)

[213] Правила пользования Сайтом ВКонтакте [Электронный ресурс] Социальная сеть «ВКонтакте». – Режим доступа: https://vk.com/terms (дата обращения 13.12.2016)

[214] Лицензионное соглашение [Электронный ресурс]. Режим доступа: Социальная сеть «Одноклассники». URL https://ok.ru/dk?st.cmd=helpContent&st.section=regulations (дата обращения 13.12.2016), Условия использования [Электронный ресурс]. Режим доступа: Социальная сеть «INSTAGRAM». URL: https://help.instagram.com/478745558852511(дата обращения 13.12.2016)

[215] Власова, Н.В., Грачева, С.А., Мещерякова М.А. Правовое пространство и человек: монография / Н.В. Власова, С.А. Грачева, М.А. Мещерякова [Электронный ресурс] // Сайт портала информационно-правового обеспечения Гарант. URL: http://base.garant.ru/57736904/#ixzz4SjGJzL35 (дата обращения 10.12.2016)

Примером борьбы с анонимностью интернет-пользователей является Китай. Так, в соответствии со ст. 10 Административных мер по безопасности и охране международных компьютерных информационных сетей (1997) частным лицам или организациям, желающим разместить в китайском сегменте какую-либо информацию, необходимо пройти у интернет-провайдера соответствующую регистрацию с указанием идентификационных данных[216]. В свою очередь интернет-провайдер обязуется проводить проверку содержания представляемой информации.

Борьба с анонимностью интернет-пользователей в Китае также выражается в контроле за деятельностью организаций, предоставляющих доступ в Интернет в специально отведенных для этого зонах (интернет-кафе, компьютерных клубах, компьютерных комнатах отдыха и т.п.)[217]. В ст. 23 регламента «Об организации работы коммерческих предприятий, предоставляющих услуги по доступу в Интернет» (2002) указано, что организации, занимающиеся коммерческой деятельностью в сфере предоставления доступа к сети «Интернет» в специально отведенных для этого зонах, должны осуществлять регистрацию удостоверения личности потребителя интернет-услуг, а также записывать соответствующую информацию по его выходу в сеть[218].

Ответственность интернет-провайдеров за размещение на своих серверах любой противозаконной информации предусмотрена национальным законодательством Бельгии[219]. Интернет-провайдер привлекается к ответственности в случае, если нет возможности привлечь самого автора размещенного материала.

Согласно § 48, 49 Закона Германии «О телекоммуникациях» нарушение требований законодательства о содержании контента на серверах, принадлежащих определенным интернет-провайдерам, является основанием для прекращения такими провайдерами своей деятельности[220].

Интересен опыт и Великобритании. В этой стране действует Фонд Интернет Наблюдения (Internet Watch Foundation - IWF), в работе которого активное участие принимают провайдеры интернет-услуг[221]. Так, при обнаружении противоправного контента в социальных сетях IWF информирует об этом интернет-провайдера, на сервере которого размещен соответствующий интернет-ресурс. В целях освобождения от уголовной ответственности такой интернет-провайдер

---

[216] Measures for Security Protection Administration of the International Networking of Computer Information Networks [Электронный ресурс]. Режим доступа: Сайт WIPO. URL: http://www.wipo.int/wipolex/ru/text.jsp?file_id=182465 (дата обращения 12.12.2016)

[217] Власова, Н.В., Грачева, С.А., Мещерякова М.А. Правовое пространство и человек: монография / Н.В. Власова, С.А. Грачева, М.А. Мещерякова [Электронный ресурс] // Сайт портала информационно-правового обеспечения Гарант. URL: http://base.garant.ru/57736904/#ixzz4SjGJzL35 (дата обращения 10.12.2016)

[218] Regulations on Administration of Business Premises for Internet Access Services [Электронный ресурс]. Режим доступа: Сайт WIPO. URL: http://www.wipo.int/wipolex/ru/text.jsp?file_id=182205 (дата обращения 12.12.2016)

[219] Власова, Н.В., Грачева, С.А., Мещерякова М.А. Правовое пространство и человек: монография / Н.В. Власова, С.А. Грачева, М.А. Мещерякова [Электронный ресурс] // Сайт портала информационно-правового обеспечения Гарант. URL: http://base.garant.ru/57736904/#ixzz4SjGJzL35 (дата обращения 10.12.2016)

[220] Telekommunikationsgesetz [Электронный ресурс]. Режим доступа: Сайт WIPO. URL: http://www.wipo.int/wipolex/ru/text.jsp?file_id=325177 (дата обращения 12.12.2016)

[221] Terms of Use [Электронный ресурс]. Режим доступа: Сайт IWF. URL: https://www.iwf.org.uk (дата обращения 12.12.2016)

незамедлительно должен либо удалить такой контент с сервера, либо блокировать доступ к интернет-ресурсу[222].

Интернет-провайдеры имеют организационно-техническую возможность в любое время воздействовать на информацию (то есть блокировать, информировать государственные органы и т.д.), поступающую от пользователей сетью, поэтому возложение ответственности на них видится целесообразным[223].

Следует также отметить, что виды ответственности к данным субъектам также различны. Например, по законодательству Швеции уголовную ответственность могут нести модераторы форумов, обязанные осуществлять мониторинг поступающих сообщений.

Определенно заслуживает внимания вопрос уголовной ответственности операторов связи и провайдеров. Однако в России говорить об их уголовной ответственности пока не представляется возможным, поскольку нет института уголовной ответственности юридических лиц.

Заключение. Одной из задач постиндустриального общества является урегулирование отношений складывающихся на просторах сети «Интернет». На сегодняшний день российское законодательство не является передовым на международной арене, а причина тому отсутствие единого мнения по данному вопросу.

Как видно из опыта зарубежных стран, возложение ответственности не только на пользователей социальными сетями, но и на интернет-провайдеров, модераторов сайтов, операторов связи, а также коммерческих организаций, предоставляющих услуги по доступу в сеть «Интернет» имеет большую перспективу. В то время как тот механизм, который существует сейчас в России, то есть возложение ответственности лишь на пользователей порождает еще большие трудности.

Как видно из рассмотренных уголовных дел, зачастую правоохранительным органам не удается даже установить ресурс, с которого была скопирована информация. Само по себе привлечение к ответственности лишь распространителя информации не нейтрализует опасности первоисточника, а, соответственно, не исключает дальнейшего его копирования и ознакомления с его содержанием.

Обсуждаемая тема многоаспектна, соответственно и решение указанных проблем не может носить односторонний характер. Вариантами их разрешения видится, в первую очередь в подключении общественности к выявлению и пресечению распространения экстремистских материалов. В частности, у такой организации как лига безопасного Интернета существует «горячая» линия для приема жалоб на Интерент-страницы, открытая для любого инициативного человека.

Ответственность организация за беспарольный Wi-Fi, безусловно, является положительной тенденцией, однако, одного этого недостаточно для ведения эффективной борьбы с распространением экстремизмом. Следует задуматься о

---

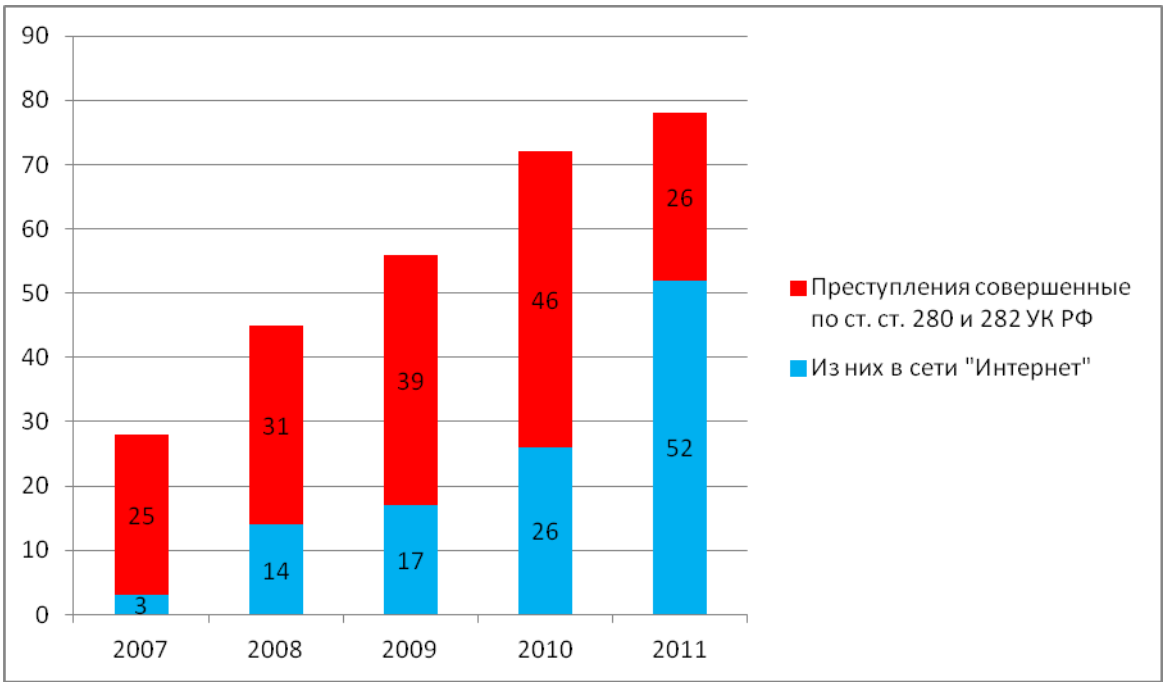
[222] Власова, Н.В., Грачева, С.А., Мещерякова М.А. Правовое пространство и человек: монография / Н.В. Власова, С.А. Грачева, М.А. Мещерякова [Электронный ресурс] // Сайт портала информационно-правового обеспечения Гарант. URL: http://base.garant.ru/57736904/#ixzz4SjGJzL35 (дата обращения 10.12.2016)

[223] Симкин, Л. Как бороться с "сетевыми" пиратами/Л. Симкин // Российская юстиция. – 2002. – N 7. – С. 63

возможности привлечения к ответственности администрации социальных сетей, ведь довольно большой процент аудитории составляют дети, которые еще в силу своего психофизического развития не способны дать объективную оценку информации, однако уже научились пользоваться современными технологиями. Сайты постоянно должны подвергаться мониторингу содержащей на нем информации, а простое перекладывание ответственности не способствует решению существующих проблем.

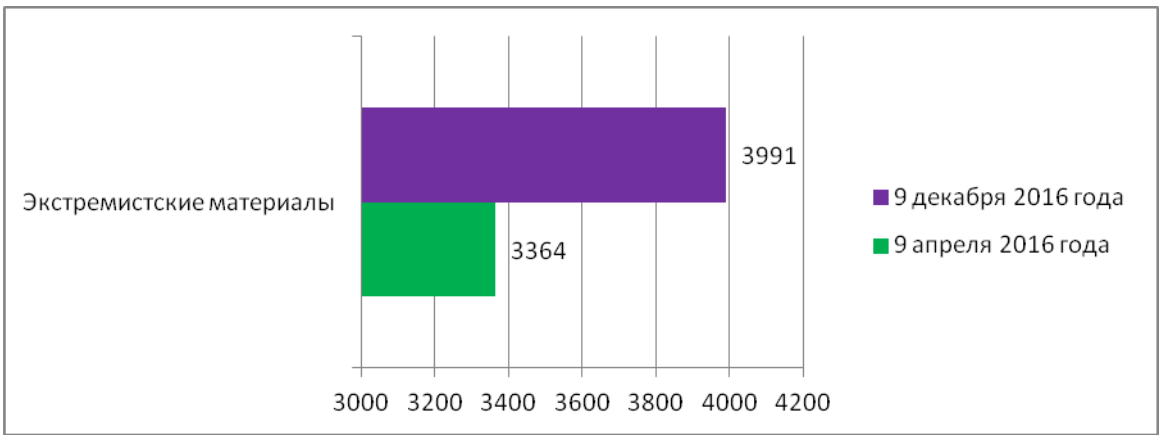
Помимо сказанного, следует повышать уровень идентификации лица в сети «Интернет», поскольку анонимность воспринимается большинством людей как безнаказанность. В этой связи назревает необходимость формирования в социальных сетях климата, основанного на неприятии информации, направленной на совершение неправомерных деяний и представляющей угрозу обществу, государству и личности[224].

Приложение 1



Федеральный список экстремистских материалов (9.04.2016 г. - 9.12.2016 г.)

[224] Власова, Н.В., Грачева, С.А., Мещерякова М.А. Правовое пространство и человек: монография / Н.В. Власова, С.А. Грачева, М.А. Мещерякова [Электронный ресурс] // Сайт портала информационно-правового обеспечения Гарант. URL: http://base.garant.ru/57736904/#ixzz4SjGJzL35 (дата обращения 10.12.2016)


Экстремистские материалы
3991
3364
3000
3200
3400
3600
3800
4000
4200
9 декабря 2016 года
9 апреля 2016 года

ПРОПАГАНДА ЭКСТРЕМИЗМА В СОЦИАЛЬНЫХ СЕТЯХ (Ермакова А.С., Габриелян А.М.).

Введение. Проблема экстремизма сегодня является очень актуальной как для мирового сообщества в целом, так и для российского общества в частности. «О необходимости принципиальной борьбы с экстремизмом заявляли и продолжают заявлять политики самых различных рангов, упуская при этом из виду то обстоятельство, что общепринятое понимание экстремизма отсутствует».[225]

В XXI веке экстремизм, переживающий эволюционный подъем, стал оказывать все большее влияние на многие сферы жизни человеческого сообщества, подрывая стабильность существования в настоящем и уверенность в завтрашнем дне. Поэтому актуальной задачей становится необходимость раскрытия сущности экстремизма, разработки понятийно-терминологического ряда, который позволил бы определить исторические, социологические, политические, психологические, информационные, силовые и другие аспекты борьбы с данным опасным явлением.

События второй половины XX века убедительно продемонстрировали, что несмотря на научно-технический и культурный прогресс, обстановка в большинстве регионов мира не стала более безопасной и стабильной. Процессы ограничения стратегических вооружений не смогли оказать сдерживающее воздействие на разработку новых видов вооружения, распространение ядерного и других современных видов оружия массового поражения.

Проблема экстремизма исследуется в отечественной и зарубежной научной литературе с древности до наших дней. На сегодняшний день, в научной литературе термин "экстремизм" раскрывается в различных аспектах, но не существует единого, комплексного междисциплинарного подхода к определению этого явления. Возможно, «основным недостатком современной литературы посвященной анализу экстремизма является довольно поверхностный, чисто криминологический характер научного подхода».[226]

Представляется, что в ряду перечисленных явлений экстремизм (от лат. exstremus – крайний) представляет особую опасность в связи с тем, что «накладываясь» на сепаратизм, национализм, фундаментализм, придает этим явлениям крайние формы их протекания, формирует реальные угрозы безопасности личности, общества, государства.

По утверждению Смолиной А.Н.: «За последние 10-15 лет понятие экстремизма перестало обозначать локальные явления из области политической практики и религиозных реформаций». Кроме того, она утверждает, что: «Экстремизм перешагнул границы маргинального явления и превратился из феномена социально-политической жизни в характерную особенность современной эпохи. Все чаще можно услышать, что мы живем в «эпоху экстремизма»: любое политическое, религиозное, социальное явление, пропагандирующее хотя бы минимальный выход за

[225] Сальников Е.В. Экстремизм как медиакатегория. Монография. – Орел, ОрЮИ МВД России, 2012.
[226] Пугачев В.П. Соловьев А.И. / Введение в политологию., АСПЕКТ ПРЕСС, - М., 2000.

пределы «толерантной» системы ценностей, объявляется СМИ «экстремистским». Однако до сих пор общее представление об экстремизме связано лишь с отдельными проявлениями экстремизма (преимущественно политического и религиозного) и «экстрима» (в основном спортивного и повседневно-развлекательного), хотя их интенсивность и возросла до степени «перехода количественных изменений в качественные». Экстремизм же как фундаментальная особенность современности пока не получил всестороннего осмысления».[227]

Актуальность нашей темы также состоит в том, что сегодня представить общество без информационного оснащения представляется затруднительным. Общество, социум, группа без информационного пространства воспринимаются как отсталые, что естественно. Проникновение информации, современных технологий и коммуникаций в жизнь простых обывателей очень велико. Информационное пространство–это еще и некая устойчивая совокупность идей, концепций, настроений, взглядов, циркулирующих в массовых коммуникационных сетях и создающих специфику информационной ситуации в том или ином регионе. Практически все без исключения социальные явления и процессы освещаются в СМИ и в Интернете. Значение последнего сегодня колоссально. Интернет можно легко использовать для достижения как положительных, так и отрицательных целей. Свобода общения и слова в интернет-среде часто становятся очень эффективным инструментом воздействия на массовое сознание в руках тех, кто преследует деструктивные цели и ставит перед собой задачи насильственного изменения нынешнего общественного порядка, если, к примеру, речь идет об экстремистах.[228]

Наша работа состоит из введения, первой главы, в которой мы рассмотрим понятие, основные проблемы и противодействие экстремизму, также из второй главы, где мы рассмотрим правоприменительную практику противодействия экстремизму в социальных сетях в России и за рубежом, и заключения.

Экстремизм в социальных сетях: понятие, проблемы, противодействие. В Федеральном законе от 25 июля 2002 г. № 114-Фз «О противодействии экстремистской деятельности» дается понятие экстремистской деятельности. Статья 1 ФЗ интерпретирует экстремистскую деятельность как:

- насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации;

- публичное оправдание терроризма и иная террористическая деятельность;

- возбуждение социальной, расовой, национальной или религиозной розни;

-пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности, или отношения к религии;

[227] http://www.slovochel.ru/
[228] Синцов Г.В. / Информационная война с экстремизмом и терроризмом, - М., 2013

- нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности, или отношения к религии;

- воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;

- воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;

- совершение преступлений по мотивам, указанным в пункте "е" части первой статьи 63 Уголовного кодекса Российской Федерации;

- пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо публичное демонстрирование атрибутики или символики экстремистских организаций;

- публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;

- публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением;

- организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;

- финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг.[229]

Существует мнение, что слово «экстремизм» происходит от латинского слова «extremus» - «крайний». В различных словарях экстремизм толкуется как приверженность к крайним взглядам и мерам. В юридической литературе понятие экстремизма может трактоваться по-разному, например, А.Г. Хлебушкин раскрывая понятие экстремизма в правовом аспекте опирается на теорию деятельности: «это противоправная деятельность, осуществление которой причиняет или может причинить существенный вред основам конституционного строя или конституционным основам межличностных отношений»[230]

Экстремизм – это деятельность общественных объединений, иных организаций, должностных лиц и граждан, основанная на приверженности крайним взглядам и

[229] Федеральный закон от 25.07.2002 N 114-ФЗ (ред. от 23.11.2015) "О противодействии экстремистской деятельности"- опубликован на Официальном интернет-портале правовой информации http://www.pravo.gov.ru - 23.11.2015

[230] Хлебушкин А.Г. Экстремизм: уголовно-правовой и уголовно-политический анализ. -Саратов, 2007. С.27

сопровождающаяся публичными насильственными и (или) противоправными действиями, которые направлены на умаление и отрицание конституционных принципов, прав и свобод человека, общества и государства. [231]

В современном обществе информационно-коммуникационные технологии глобальная сеть Интернет и стали ключевыми факторами развития отдельных государств и формирования единого информационного пространства. Широкое распространение новых технологий, наряду с положительными аспектами (возможность поиска и передачи различной информации (электронные библиотеки, информационные БД, НПА и т.д.), новые коммуникационные возможности (E-mail, ICQ, Skype и т.д.), оказывает негативное воздействие на различные социально-экономические и политические процессы.

Пожалуй, сейчас очень сложно найти человека, не знакомого с термином «социальная сеть». Технически, социальная сеть является объединением группы людей на одной Интернет-платформе, позволяющей пользователю загружать свою личную информацию и обмениваться им с другими пользователями. Возможности общения пользователей по публикации и обмену контентом отличают социальные сети от других Интернет-ресурсов. Немаловажной чертой социальных сетей является высокий уровень интерактивности, при котором скорость обмена контентом и скорость общения зачастую не уступают общению вне сети.

Экстремизм в молодежной среде – один из самых опасных и сложно прогнозируемых феноменов современности, способный распространять свое влияние на различные сферы общественной жизни. Экстремизм превратился в весомый фактор дестабилизации социально-экономической и политической ситуации в мире. Неудивительно, что специфика его проявлений привлекает внимание представителей различных социогуманитарных наук, которые подчеркивают системный и многоаспектный характер этого явления.[232]

Федеральный закон от 23.11.2015 №314 ФЗ:

1) экстремистская деятельность (экстремизм): пропаганда и публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо публичное демонстрирование атрибутики или символики экстремистских организаций;

2) публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;

3) экстремистские материалы – предназначенные для обнародования документы либо информация на иных носителях, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том

[231] Истомин А.Ф., Лопаткин Д.А. К вопросу об экстремизме // Современное право. Новое в российском законодательстве: обзоры, комментарии, практика 2005. №7.

[232] Молодежный экстремизм в социальных сетях: специфика и теоретическое осмысление / В. В. Котлярова, М. М. Шубина, О. Н. Сысоева // Alma mater (Вестник высшей школы). - 2016. - № 5. - С. 95-99.

числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии, публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное ничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы.[233]

В настоящее время социальные сети зачастую действуют в симбиозе с традиционными СМИ, играя роль распределителя готового контента. Помимо распределительной функции, социальные сети зачастую исполняют роль информагентства, предоставляя СМИ информацию, на основании которой и создается готовый новостной и аналитический контент. В качестве примера можно отметить частое появление роликов с видеохостинга Youtube.com в новостных и аналитических передачах центральных телеканалов.

Естественно, что столь мощный медийный инструмент имеет свою специфику и может быть использован для публикации материалов экстремистской направленности. Если новостное Интернет-издание публикует материал экстремистской направленности, то у государства есть эффективные рычаги воздействия в виде УК РФ и единого списка экстремистских материалов, посредством которых можно достаточно оперативно ограничить доступ Интернет-пользователей к вышеуказанным материалам, а в некоторых случаях даже ограничить доступ к самому сайту, на котором они опубликованы. Социальные сети контролировать гораздо сложнее, нежели обыкновенные Интернет-сайты.

Пропаганда экстремизма в социальных сетях, помимо особенностей, изложенных выше, имеет свою специфику. Ввиду того, что в социальных сетях часто указывается личная информация, возможно целенаправленное распространение материалов, реклама групп, например, для определенной возрастной группы пользователей для оказания максимального на них влияния. Для религиозного экстремизма в качестве примера можно рассмотреть возрастной состав любой группы, пропагандирующей религиозный фундаментализм. Средний возраст подписчиков невысок, более половины составляет молодежь до 18 лет, что и представляет благодатную почву для продвижения идей религиозного экстремизма из-за внушаемости данной группы лиц.

Для эффективной борьбы с пропагандой экстремизма в социальных сетях необходимо наличие действенного механизма по осуществлению непрерывного мониторинга и оперативного блокирования вредоносного контента и принятия мер в рамках законодательства РФ в отношении лиц, распространяющих данный контент.

Зачастую требуется незамедлительно ограничить доступ пользователей социальных сетей к контенту, содержащему призывы к экстремистским действиям, однако для этого требуется дождаться окончания официальной процедуры по

[233] Федеральный закон от 23.11.2015 N 314-ФЗ "О внесении изменения в Федеральный закон "О противодействии экстремистской деятельности"- официальный интернет-портал правовой информации http://www.pravo.gov.ru, 23.11.2015

признанию его экстремистским, т.е. решения суда и внесения страницы в единый реестр экстремистских сайтов. Но данная процедура не должна становиться элементом цензуры, нарушая конституционные права граждан РФ.

В зависимости от вида преступлений экстремистской направленности сети Интернет могут быть использованы для:

1.распространения экстремистских материалов (публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма и др.);

2. обеспечения деятельности экстремистских сообществ, организаций (склонение, вербовка или иное вовлечение лиц в совершение преступлений экстремистской направленности, руководство сообществом, организацией, его частью, разработки планов, условий для совершения преступлений экстремистской направленности, связи, инструктажа участников и т.п.).

Чаще всего при помощи сети Интернет совершаются публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ), так как их размещение в сети не представляет особых сложностей. Важнейшим признаком, влияющим на квалификацию данного деяния, является публичность призывов, которая означает, что они обращены к широкому кругу лиц, т.е. ко всем пользователям сети Интернет и преследуют цель вовлечения в экстремистскую деятельность как можно большего количества людей. Характерной чертой данного преступления является отсутствие действий по подстрекательству конкретного лица совершить определенное преступление. По конструкции объективной стороны состав – формальный, окончен с момента распространения таких призывов через сеть Интернет. Не имеет значения - вовлечены лица в экстремистскую деятельность или нет.

Через Интернет может происходить возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ). Эта норма основана на ч. 2 ст. 29 Конституции РФ, в которой провозглашается недопущение пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду, а также запрета пропаганды социального, расового, национального, религиозного или языкового превосходства.

Объективная сторона характеризуется действиями, направленными на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, если эти деяния совершены публично или с использованием средств массовой информации. Сделать это можно с помощью пропаганды в Интернете путем систематических призывов, направленных на внедрение в общественное сознание идей и формирование установок. Поэтому к данному признаку нельзя отнести единичные высказывания и суждения, выдвинутые в качестве тезиса в дискуссии (например, высказывания участников интернет-форумов).

Например, это могут быть призывы, вызывающие длительное состояние враждебности между значительными группами людей в зависимости от

национальной или расовой принадлежности или отношения к религии (депортация, применение насилия, воспрепятствование проведению национальных или религиозных обрядов и т.п., а равно призывы к совершению названных и других подобных действий). Кроме того, состав охватывает действия, направленные на издевательство над историей, культурой, обычаями и традициями какой-либо нации и т.п. В этом случае направленность действия на унижение национального достоинства небольшой группы или даже отдельных представителей определенной нации определяется именно его принадлежностью к данной нации. Пропаганда исключительности или неполноценности предполагает пропаганду не в отношении отдельных представителей этнических групп или религиозных конфессий, а в целом этих групп или конфессий.

Общим и обязательным признаком для всех описанных деяний является то, что они совершаются либо публично (включая сеть Интернет), либо с использованием средств массовой информации.

Состав также формальный, окончен с момента помещения в Интернете соответствующей информации.

Через Интернет может быть организовано экстремистское сообщество (ст. 282.1 УК РФ), например, путем сговора и приискания соучастников. Деяние включает, прежде всего, создание экстремистского сообщества, т.е. организованной группы для подготовки или совершения преступлений экстремистской направленности. При квалификации необходимо учитывать, что законодателем экстремистское сообщество определено в ч. 1 ст. 282.1 УК РФ через такую форму соучастия как организованная группа. Следует присоединиться к высказанному мнению о том, что, создаваясь для совершения преступлений экстремистской направленности, такое сообщество воспринимается как разновидность преступной организации. Поэтому при той ситуации, когда преступное сообщество наряду с общеуголовными преступлениями станет планировать и совершение деяний, содержащих признаки экстремизма, это должно повлечь уголовно-правовую оценку содеянного по совокупности ст. 210 и ст. 282.1 УК РФ[234].

Способы использования сети Интернет в экстремистских целях могут быть следующими:

1. Сбор с помощью Интернета подробной информации для совершения преступлений экстремистской направленности;

2. Сбор денег для поддержки экстремистских движений;

3.Создание сайтов, содержащих сведения о лицах, поддерживающих экстремизм, их целях и задачах, публикация на этих сайтах данных о времени и встрече заинтересованных лиц;

4. Использование Интернета для: информационно-психологического воздействия, обращения к массовой аудитории для сообщения о будущих и уже

[234] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 22.11.2016) // "Российская газета", N 113, 18.06.1996, N 114, 19.06.1996, N 115, 20.06.1996, N 118, 25.06.1996.

спланированных экстремистских действиях, рассылки подобных сообщений по электронной почте и т.д.

5.Вовлечение в совершение данных деяний лиц, умыслом которых не охватывается совершение преступлений экстремистской направленности - например, хакеров, которым неизвестно, к какой конечной цели приведут их действия.

Опасность Интернет-экстремизма состоит в том, что он не имеет территориальных границ, поэтому деяния экстремистской направленности могут осуществляться из любой точки мира. Как правило, обнаружить виновных в информационном пространстве сети Интернет очень сложно, так как они действует через один или несколько компьютеров с измененными (с помощью специального программного обеспечения) IP-адресами, что затрудняет его идентификацию и определение местоположения и обеспечивает высокую степень анонимности. Ряд сайтов экстремистских и взаимодействующих с ними террористических формирований создают сайты-«однодневки», меняют их форматы и адреса, что существенным образом затрудняет работу по документированию их незаконной деятельности в электронном пространстве.

Информация об использовании сетей Интернет в целях совершения преступлений экстремистской направленности может быть получена в результате проведения оперативно-розыскных мероприятий, при явке лица с повинной, из поступивших заявлений, сообщений граждан, общественных организаций, государственных органов, средств массовой информации и иных источников.

В большинстве случаев факты совершения указанных противоправных действий устанавливаются сотрудниками правоохранительных органов.

При получении сообщения о возможном совершении преступления экстремистской направленности проводится доследственная проверка с целью уточнения и объективного подтверждения фактов, изложенных в заявлениях, сообщениях, иной поступившей информации.

В процессе такой проверки устанавливаются:

- места неправомерного проникновения в компьютерные сети (внутри потерпевшей организации или извне) либо распространения экстремистских материалов, способы преодоления информационной защиты (подбор либо знание паролей, отключение средств защиты (в том числе извне), использование несовершенств такой защиты, применение специальных программных средств);

-содержание и назначение информации, подвергшейся воздействию либо распространенной в сетях Интернет, ее отнесение экстремистским материалам;

- размер ущерба, причиненного в результате противоправных действий;

-средства, использованные при совершении противоправных действий (технические, программные, комбинированные);

- принадлежность IP-адресов и доменных имен;

- места изготовления вредоносных программ или экстремистских материалов;

- причастность конкретных лиц к совершению уголовно-наказуемых деяний, а также цели, мотивы при осуществлении ими своих действий;

- наличие причинной связи между неправомерными действиями и наступившими последствиями.

Использование компьютерных сетей для совершения преступлений экстремистской направленности характеризуется тем, что не остается видимых следов преступления. В связи с этим осложнены поисковые мероприятия, сбор доказательственной информации. В этих случаях целесообразно привлекать в качестве специалистов лиц, обладающих специальными познаниями в области разработки программного обеспечения и компьютерной техники, которые могут найти и определить способы размещения, пересылки информации в сетях Интернет, установить следы использования компьютерной и иной оргтехники.

По результатам пленума Верховного суда стало понятно, что вскоре законодательство в отношении экстремистской деятельности будет ужесточено. Отдельно внимание будет уделено распространению соответствующих идей в Интернете. Экстремизм в социальных сетях процветает – это уже понятно всем, и настало время бороться с ним.

Уже не раз люди уголовно наказывались за публикацию экстремистских материалов в социальных сетях. В будущем рассылка их с использованием данных каналов также станет подсудным делом. Иными словами, личные сообщения будут приравнены к публичным постам.

Что касается вербовки, то здесь все зависит от того, поддастся ли пользователь социальных сетей на уговоры «рекрутера». Если после подобного разговора он совершит преступление, то факт склонения к экстремистской деятельности будет подтвержден. Если нет – то и ответственности не будет.

Много споров вызывали случаи, когда публикация материала уголовно преследовалась независимо от ее контекста. Обновленное законодательство будет учитывать, что именно хотел сказать автор поста в социальной сети.

Бывает такое, что люди приводят цитату из экстремистского материала в качестве примера или с целью осуждения соответствующей деятельности. За это судить не будут. Максимально помогать в этом деле будут комментарии, выражающие точку зрения автора поста.

Основные детерминанты, приоритетные направления экстремизма в социальных сетях и современная практика его противодействия. За последние годы виртуальные социальные сети стали самым массовым и перспективным средством коммуникаций. По оценкам различных исследовательских центров, самой распространенной среди молодежи является виртуальная социальная сеть ВКонтакте. Согласно данным сервиса статистики ВКонтакте, в октябре 2016 года число зарегистрированных пользователей по всему миру составило 239 млн. человек.

Развитие экстремизма в Интернете представляет особую опасность, потому что интернет-пространством пользуются как взрослые люди, так и дети и экстремистские группировки сознательно влияют на общество путём пропаганда экстремистских материалов для манипуляций политических сил.

На сегодняшний день, в научной литературе существуют экспериментально подтвержденные данные негативного влияния материалов экстремистской направленности, размещенных, в том числе, в социальных сетях, на молодежь. А.А. Оселковым было проведено экспериментальное исследование с целью изучения психологических особенностей влияния материалов экстремистской направленности на молодёжную аудиторию. Результаты исследования свидетельствуют о том, что тексты, содержащие прямую пропаганду экстремизма, способствуют формированию негативного образа определённых социальных групп, повышению уровня открытого проявления агрессии, сильному снижению уровня позитивных эмоций и повышению негативных, а также активации установок на действия против указанных групп.[235]

Способы вовлечения молодых людей в экстремистские организации с помощью Интернета довольно многогранны использующие разные способы воздействия на личность, ценности и мировоззрение. На начальном этапе экстремистские группы могут привлекать молодого человека своей оригинальностью, альтернативностью, агрессивностью жизненного стиля. Однако затем, попадая под влияние данных объединений, молодые люди нередко подвергаются физическому и психическому принуждению, происходит ломка личности молодого человека, замена ценностных ориентаций.

Можно выделить несколько причин, в силу которых использование сети Интернет экстремистских организаций являются действенными в отношении молодежи:

1.Легкость и быстрота распространения информации в сети Интернет, т.к. социальные сети и форму очень популярны среди молодежи.

2.Высокая анонимность общения (использование множества анонимизирующих программ, использование иностранных доменов и серверов).

3.Минимальный контроль со стороны государственных структур.

4.Возможность быстрой ликвидации информационной базы.

Особенности распространения информации в социальных сетях определяют их значение, которое трудно переоценить. Информационный экстремизм характеризуется следующими общими и специфическими параметрами:

- радикальностью (экстраординарностью) действий в достижении каких-либо целей, реализации интересов;
- антисоциальностью, поскольку нарушает исторически сложившиеся (типичные), позитивные формы и модели социально-правового взаимодействия;
- аморальностью, так как всегда идет в разрез с духовно-нравственными нормами;
- институциональностью, он «вызревает» и институционализируется в пограничных условиях и маргинальных пространствах;

[235] *Оселков А.А.,* Психологические особенности влияния на студентов высших учебных заведений материалов экстремистской направленности: автореф. дис..канд. психол. наук. – Ростов-на-Дону, 2011.

- искажением политико-правового мышления, поскольку субъект экстремистской деятельности обладает чаще всего деформированным сознанием, что обусловливает его отчуждение от социально-культурных и политико-правовых норм и ценностей;
- противоправностью результатов, поскольку функционирование информационного экстремизма в ряде случаев соответствует закону, но реализует предоставленные возможности в противоположных целях.

Социальные сети контролировать гораздо сложнее, нежели обыкновенные Интернет-сайты. Российская социальная сеть «Вконтакте», по заявлениям ее пресс-службы, активно сотрудничает с органами внутренних дел в плане удаления экстремистских материалов и прочим направлениям, но, несмотря на это, сеть изобилует группами, которыми ведется открытая пропаганда религиозного экстремизма и фундаментализма, группами, размещающими материалы, которые можно причислить к политическому экстремизму, например, выступающими за нарушение территориальной целостности РФ. Однако данные группы остаются без внимания и если группу, выступающую, к примеру, за выход Сибири из состава РФ, теоретически можно закрыть по предписанию прокуратуры, то с группами, ведущими пропаганду религиозного экстремизма, дело обстоит сложнее. Несмотря на достаточно широкое определение понятия экстремизма в УК РФ, публикуемые материалы не признаются экстремистскими в ходе экспертиз, либо они о них не становится вовремя известно внутренним органам.

Зарубежные социальные сети находятся вне поля российского законодательства, потому фактически они являются открытой площадкой для публикации материалов экстремистской направленности.

Согласно Давыдову В. О. существуют два способа «совершения экстремистских преступлений с использованием компьютерных сетей», которые включают в себя две основные группы:

1)изготовление и распространение (манипулирование) посредством телекоммуникационных сетей и, в первую очередь, глобальной сети Интернет, информационной продукции, запрещённой российским законодательством и противоречащей интересам национальной безопасности государства в целях оказания информационно-психологического воздействия на массовые аудитории граждан;

2) использование компьютерной техники и информационных технологий в целях организации и последующего руководства деятельностью экстремистских групп и сообществ, а также создания условий для совершения преступлений экстремистской направленности. [236]

Опасность коммуникационных технологий заключается в том, что выдавая за «обмен мнениями» экстремисты ведут пропагандистскую деятельность, занимаются вербовкой, тем самым увеличивают количество сторонников своей идеологии, и при

[236] Давыдов, В.О. Методика расследования экстремистских преступлений, совершенных в компьютерных сетях. / В.О. Давыдов. – М.: Юрлитинформ, 2014. – С.33.

этом способствуя установлению контактов с группами экстремистского характера по всему миру.

Экстремистские материалы на сайтах размещают в различных формах: нацистская символика соответственно и нацистская литература; карикатуры, в основном высмеивающие, принижающие представителей Кавказа, Средней Азии, мигрантов; это могут быть демотиваторы, направленные против определенных кругов власти и народов и т. д. Такого рода материалы можно найти на страницах групп: «Академия порядочных скинов»[237]; «Славянская сила — Nord West Peterburg»[238], «Русская зачистка»[239] и т. д.

Помимо информационной функции социальные сети выполняют и функции по организации и координации массовых акций, имеющих своей целью открытую конфронтацию законно избранной власти. Задачи, которые решают руководители экстремистских групп через социальные сети заключаются в том, чтобы «обольстить» пользователей, создав с помощью информационно — манипулятивных техник максимально привлекательный образ своего сайта, сформировать или пробудить желание стать участником группы. [240]

Один из самых используемых приемов — заведомо ложное истолкование истории. Этот метод нацелен на постепенное изменение общественного мировоззрения. Распространяется миф о многовековой и непрекращающейся войне кавказских народов с Россией. Искажению подвергаются и факты сравнительно недавней истории. Еще один популярный прием — создание эффекта присутствия. Он достигается за счет размещения на веб-сайтах видеороликов якобы с «места боевых действий». Так, на сайте «Кавказ-центр» были размещены видеообращения боевиков к молодежи с призывами к вооруженным действиям и террористическим актам, угрозами в адрес «оккупантов» и «национал-предателей».

Также часто используется гиперболизация негативных черт и неудач противника. Намеренно рисуется неприглядный образ России. На интернет-сайтах «Кавказ-центр», «Кавказ-монитор» фигурировали такие заголовки статей, как «Российская экономика на грани коллапса», «Россия — лжевеликая держава», «Четверть населения России психически больная».[241]

Наконец, довольно распространенным приемом экстремистских интернет-ресурсов является фактографическая пропаганда, когда под видом беспристрастных новостей преподносится, по сути, политически ориентированная информация. То есть экстремисты не только ставят под сомнение точность информации, поступающей из российских источников, но и пытаются популяризировать принятые в их среде географические названия, имеющие выраженную идеологическую окраску.

---

[237] «Академия порядочных скинов» //https://vk.com/colub95960921
[238] «Славянская сила — Nord West Peterburg» //https://vk.com/club60982278
[239] «Русская зачистка» https://vk.com/event97221492
[240] Салахутдинов А. А. Социальные сети как информационный канал экстремистского материала // Молодой ученый. — 2014. — №17. — С. 561.
[241] Литвинова Т. Н. «Информационный джихад» в глобальной сети // Власть. 2010. №9.

Обобщая вышесказанное, следует отметить, что виртуальные социальные сети представляют собой самое массовое и легкодоступное средство коммуникации, что порождает целый ряд проблем, связанных с негативным влиянием националистических экстремистских материалов, распространяемых в виртуальных сообществах.

Законотворческая и правоприменительная практика противодействия экстремизму в социальных сетях в Современной России и в Зарубежных странах. Важным фактором в предупреждении молодежного экстремизма является формирование на федеральном уровне стратегии государственной молодежной политики.

В стране разработаны и внедрены в практику учреждений культуры, образования, охраны правопорядка многочисленные нормативно-правовые документы, регулирующие профилактику экстремизма в молодежной среде федерального и регионального уровней, в том числе Кодекс РФ от 20.12.2001 № 195-ФЗ «Об административных правонарушениях»[242]; Федеральный закон от 06.10.2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации»[243]; Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»[244] и многие другие документы. Вместе с тем анализ существующих программ по противодействию идеологии экстремизма позволяет констатировать односторонность подходов к решению проблемы, недостаточную разработанность системы превентивных мер, интегрирующих сегменты государственно-правового регулирования, развития культуры и образования, оптимизации функционирования СМИ, совершенствования социально-культурной деятельности. Особо остро эти проблемы ощущаются на региональном и муниципальном уровнях, поскольку осуществление конкретных мер по противодействию идеологии и практике экстремизма возложено на органы местного самоуправления, государственные учреждения и общественные организации, действующие на конкретной территории. [245]

Имеющийся зарубежный опыт свидетельствует о целесообразности создания при участии компаний, оказывающих услуги в сети Интернет, наблюдательных советов и «горячих линий», которые были бы наделены полномочиями оперативно удалять из глобальной сети материалы, содержащие экстремистскую направленность, как это узаконено в большинстве развитых стран. Глобализация информационно-коммуникационной среды не только изменила облик социума, но и оказала существенное влияние на молодежную среду. Научно-техническая революция, внедрение в общественную жизнь инновационных информационных технологий

[242] Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 22.11.2016) // СПС Консультант Плюс.
[243] Федеральный закон от 06.10.2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» от 30.12.2001 N 195-ФЗ (ред. от 22.11.2016) // СПС Консультант Плюс.
[244] Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» от 25.07.2002 N 114-ФЗ (действующая редакция, 2016) // СПС Консультант Плюс.
[245] Кузьмин А.В. Социально-культурная профилактика экстремизма в молодежной среде: автореф. дис. … д-ра пед. наук. – Тамбов, 2012.

привели как к позитивным, так и негативным эффектам. В частности, информационное неравенство, виртуализация образа жизни, развитие информационных сети Интернет могут рассматриваться и в качестве факторов молодежного экстремизма. Отмеченные негативные социокоммуникативные эффекты способствуют трансформации молодежного экстремизма, оптимизируют его адаптацию к новым условиям социальной реальности.

Опыт международной антитеррористической деятельности позволяет сформулировать первоочередные задачи по борьбе с терроризмом и экстремизмом в сети Интернет:

– разработать научно-методическое обеспечение по пресечению террористических атак с использованием глобальных информационных сетей, выработать единый понятийный аппарат, шкалу оценки угроз и их последствий;

– выработать механизм взаимного информирования о широкомасштабных компьютерных атаках и крупных инцидентах;

– выработать способы совместного реагирования на угрозы терроризма;

– унифицировать национальные законодательства в сфере защиты критической инфраструктуры от интернет-терроризма. Информационная контртеррористическая война – это объективная реальность. И поэтому надо быть готовым не просто к модернизации приемов противоборства, а к созданию и использованию опережающих технологий.

Особую актуальность приобретает вопрос наличия в российском законодательстве необходимых средств для борьбы с проявлениями экстремизма в Интернете. До середины 2012 г. корпус законодательства, который можно было использовать для регулирования интернет-контента, включал в себя федеральные законы «О связи»[246], «Об информации, информатизации и защите информации»[247], а также закон «О СМИ»[248]. Боролись с экстремизмом в Интернете, используя соответствующие нормы в уголовном законодательстве – о призывах к экстремистской деятельности (ст. 280 УК), возбуждении ненависти (ст. 282 УК), а также о публикациях, которые могут быть отнесены к деятельности экстремистского сообщества (ст. 282.1 УК) или запрещенной организации (ст. 282.2 УК).[249] Также использовались нормы КоАП – ст. 20.3 «Пропаганда и публичное демонстрирование нацистской атрибутики» и ст. 20.29 КоАП РФ «Производство и распространение экстремистских материалов».[250] Практика последних лет показала, что борьба с экстремизмом за последние четыре года активно стала переходить из реального мира в онлайн. В 2015 году в России за экстремистскую деятельность или призывы к

[246] Федеральный закон "О связи" от 07.07.2003 N 126-ФЗ (действующая редакция, 2016) // СПС Консультант Плюс.
[247] Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (действующая редакция, 2016) // СПС Консультант Плюс.
[248] Закон РФ от 27.12.1991 N 2124-1 (ред. от 03.07.2016) "О средствах массовой информации" (с изм. и доп., вступ. в силу с 15.07.2016) // СПС Консультант Плюс.
[249] Уголовный кодекс Российской Федерации N 63-ФЗ от 13.06.96 // СПС Консультант Плюс.
[250] Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 22.11.2016) // СПС Консультант Плюс.

экстремизму осудили 544 человек; еще 110 человек — за терроризм и призывы к нему. Такие данные содержатся в опубликованном Судебным департаментом при Верховном суде Российской Федерации документе «Основные статистические показатели деятельности судов общей юрисдикции в 2015 году». По сравнению с 2014 годом количество осужденных по экстремистским статьям увеличилось более чем на четверть (этот показатель составлял 414 человек). Больше всего обвинительных приговоров — по 122 — вынесено в Центральном и Приволжском федеральном округах. В Сибири осуждено за экстремизм 70 человек, в Северо-Западном федеральном округе — 60, в Южном федеральном округе — 54, в Северо-Кавказском — 32, в Уральском — 31, на Дальнем Востоке — 29 человек. Пять человек осудили по делам об экстремизме в Крыму.[251]

Рассмотрим, несколько, актуальных на сегодняшний день, экстремистских дел. Так против краснодарской ЛГБТ-активистки Нины Соловьёвой было возбуждено дело за публикацию в соцсети «ВКонтакте» ролика с песней Бориса Севастьянова «Это, детка, рашизм». 7 апреля 2016 года Соловьёва обжаловала в краевом суде решение Октябрьского районного суда Краснодара, отправившего ее под арест на десять суток по административной статье о демонстрации нацистской символики.

В Курске 14 апреля состоится судебный процесс над интернет-активистом за размещение записей в соцсети «ВКонтакте» — Сергею Лаврову предъявлено обвинение по ч. 2 ст. 280 УК РФ (Публичные призывы к осуществлению экстремистской деятельности). Сергей Лавров стал фигурантом уголовного дела в 2015 году за размещение видеоролика и других записей в группе под названием «Российский спецназ оппозиции им. Чапаева». Дело расследовало управление ФСБ. По версии обвинения, у молодого человека «возник преступный умысел на публичные призывы к осуществлению насильственного изменения государственного строя России путем революции».

Самым громким происшествием в 2016 году, вызвавшим большой общественный резонанс, стало дело екатеринбургского видеоблогера Руслана Соколовского. Видеоблогер, 3 сентября 2016 был задержан правоохранительными органами Екатеринбурга по обвинению в экстремизме и оскорблении чувств верующих. Поводом для возбуждения уголовного дела послужило видео, опубликованное 11 августа на канале YouTube Соколовского, в котором он ловит в храме покемонов через приложение для смартфонов Pokemon GO. К оскорблению чувств верующих следователи отнесли не сам факт игры на территории церкви, а те высказывания, которыми Соколовский сопровождал этот процесс. Подобным образом в уголовном деле фигурируют и другие видеофайлы, также размещенные от имени этого же блогера в разное время в 2016 году".

Как уточнили в ведомстве, экспертной оценке специалистов в области лингвистики, религиоведения и психологии были подвергнуты три видео, в двух из которых эксперты однозначно усмотрели признаки экстремизма.

[251] Официальный сайт Судебного Департамента при Верховном Суде в Российской федерации // URL: http://www.cdep.ru/index.php?id=79

Таким образом, ведется активная борьба против экстремизма в Интернете, но открытым остается вопрос эффективности данной работы. Для того чтобы задача борьбы против экстремизма была успешно решена, необходим целый ряд комплексных мер, предусматривающих проведение эффективной социальной политики, формирование продуманной системы политического воспитания граждан, особенно молодежи, создание социально направленной правовой системы.

Заключение. Современный молодежный экстремизм детерминирован появлением нового уровня проблемных вопросов социального, психологического, политического, информационного, экономического, управленческого и иного характера.

Эта насущная проблема требует своего решения, тем более что экстремистские и террористические организации активно применяют новейшие суггестивные технологии для вовлечения в свои ряды молодежи.

Важно не только более четко выявить круг причин, вызывающих экстремистские проявления в молодежной среде в результате общения в социальных сетях, но и предусмотреть меры, снижающие риск таковых. Искать рациональную основу экстремистских действий бессмысленно, поскольку в основе экстремизма лежат эмоции и конформизм.[252]

Императивные исследования интернет-опроса показали, что большая часть опрошенных сталкивались с экстремистскими материалами в социальных сетях, но ещё больший процент опрошенных не знают, как поступить и куда обращаться в случае обнаружения таких материалов. Что является одной из наиболее острой проблемой.

Причину наличия экстремистских материалов в социальных сетях по результатам опроса однозначно определить невозможно. Выделили три наиболее явные причины, это: лёгкость и быстрота распространения информации в сети Интернет, высокая анонимность общения и минимальный контроль со стороны государственных органов. А проблему решения данной ситуации наибольшее количество человек считают - привлечение к работе по профилактике экстремистской деятельности наиболее популярных блогеров, готовых к диалогу и взаимодействию в противоборстве экстремизму.

В итоге можно сделать вывод о том, что для российского Интернет-пространства необходимо наличие структур, которые могут успешно осуществлять мониторинг социальных сетей и своевременно информировать правоохранительные органы о фактах пропаганды политического и религиозного экстремизма. Это позволит существенно повысить эффективность по противодействию экстремизму, не давая заинтересованным лицам вести пропаганду и распространение экстремистских материалов.[253]

---

[252] Молодежный экстремизм в социальных сетях: специфика и теоретическое осмысление / В. В. Котлярова, М. М. Шубина, О. Н. Сысоева // Alma mater (Вестник высшей школы). - 2016. - № 5. - С. 95-99.

[253] Химилонова М.Т. «Социальные сети: экстремизм и терроризм».- Владикавказ, 2016

На наш взгляд, одним из путей снижения уровня потенциальной угрозы виртуальных социальных сетей как средства коммуникации является разработка комплексных мер государственного контроля ресурсов социальных сетей, а также технологий отслеживания и блокирования виртуальных сообществ, имеющих экстремистскую направленность.

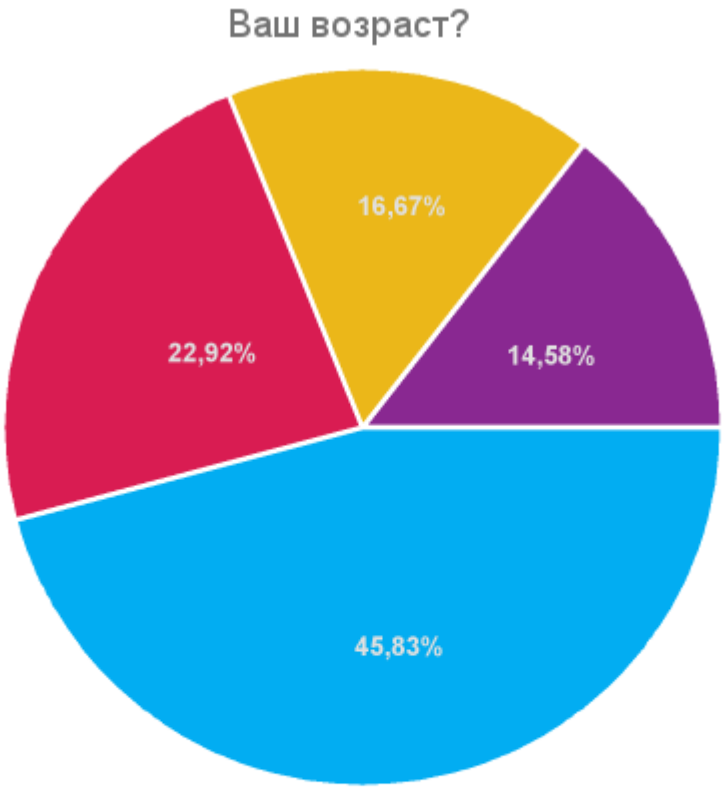
Некоторые меры предосторожности: Прекратите контакты с пользователями, имеющими на своих страницах в социальных сетях и блогах специфическую символику (свастика, символы фашистской Германии, изображение фашистского приветствия (приветствие римских легионеров) и т.п.; использующих специфические наименования, термины, обозначения и словосочетания («фашист», «нацист», «скинхед» и т.п.); специфические унизительные или ругательные наименования и определения представителей какой-либо национальности («чернокожий», «азер» и т.п.); специфический сленг или лексикон, распространенный в среде экстремистских формирований («русофоб», «ZOG» и т.п.); специфические имена и клички известных и авторитетных лиц в конкретных радикальных движениях («Лимонов», «Тесак» и т.п.); использующих специфическихе «ники» при написании интернет-материалов («Фюрер», «White warrior», «Геринг» и т.п.); именные наименования существующих экстремистских группировок («Сварожичи», «Русский кулак» и т.п.).

Что делать если вам предлагают заняться экстремистской деятельностью? Главное не соглашаться, никакие доводы и уговоры не должны зародить в вас сомнения. Обязательно запомните данные того человека от которого поступило предложение, если нет конкретных данных (ФИО), т.к. чаще всего пользуются псевдонимами или подставными именами, то запишите электронный адрес или любые данные полученными от человека. Далее следует проявить свою активную гражданскую позицию, и помочь сотрудникам правоохранительных органов пресечь данные действия.

В общении, и в сети Интернет в том числе, помните: Понимание культуры и традиций другой национальной группы - источник конструктивного межнационального сотрудничества. С целью налаживания отношений между разными этническими и национальными группами: 1) относитесь к чужой культуре с тем же уважением, с которым относитесь к собственной; 2) не судите о ценностях, убеждениях и традициях других культур отталкиваясь от собственных ценностей; 3) никогда не исходите из превосходства своей религии над чужой религией; 4) Общаясь с представителями других верований, старайтесь понимать и уважать их точку зрения; 5) Помните, что каждая культура, какой бы малой она не была, имеет что предложить миру, но нет такой культуры которая бы имела монополию на все аспекты; 6) Всегда помните, что никакие научные данные не доказывают превосходство одной этнической группы над другой.

7) Если вы с чем-то не согласны, не переходите на оскорбления, не используйте слова, которые унижают честь и достоинство другого. Будьте толерантны.

Результаты опроса “Экстремизм в Социальных сетях”



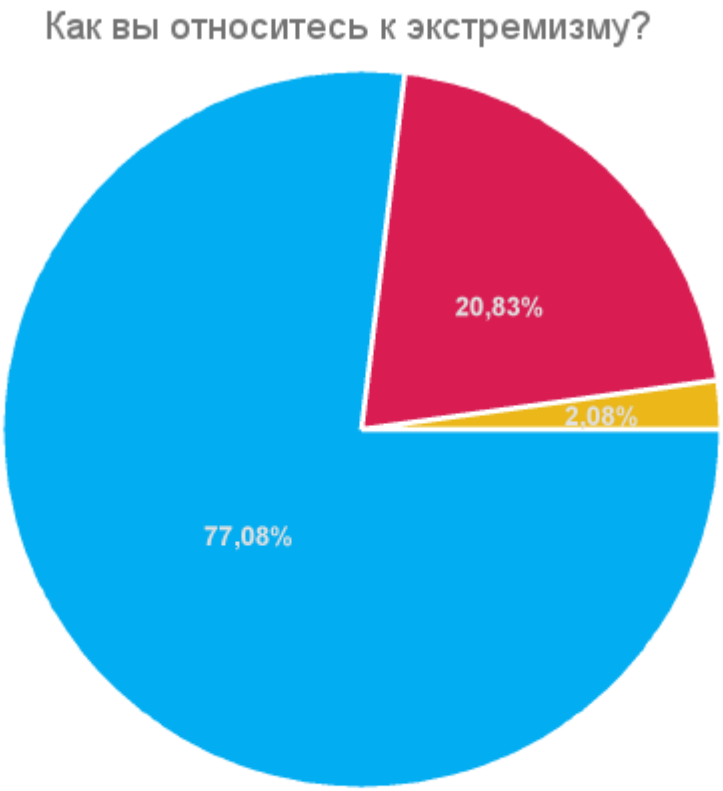
18-22	45,83%	22
22-30	22,92%	11
до 18	16,67%	8
старше 30	14,58%	7

Testograf.ru

Да, знаю	79,17%	38
Затрудняюсь ответить.	18,75%	9
Нет, не знаю	2,08%	1

Testograf.ru

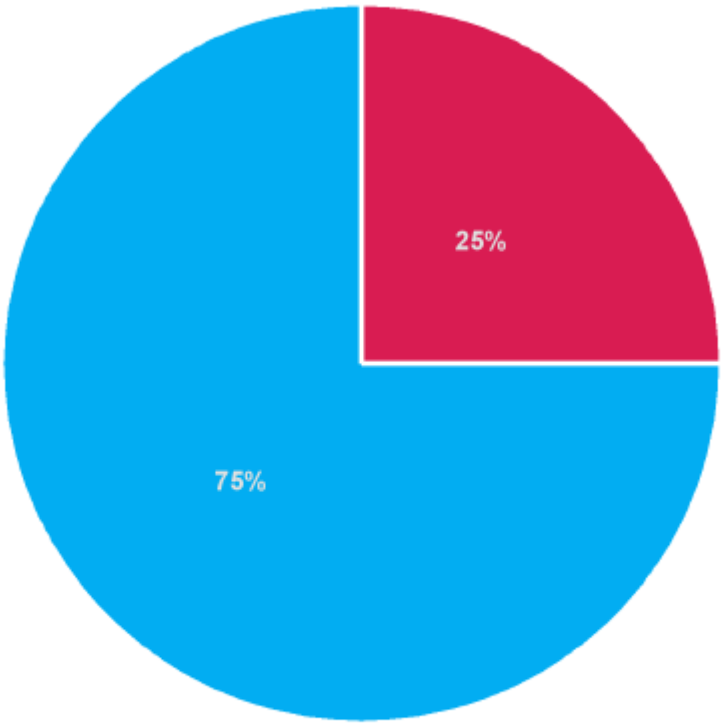
2.



Негативно	77,08%	37
Нейтрально	20,83%	10
Положительно	2,08%	1

Testograf.ru

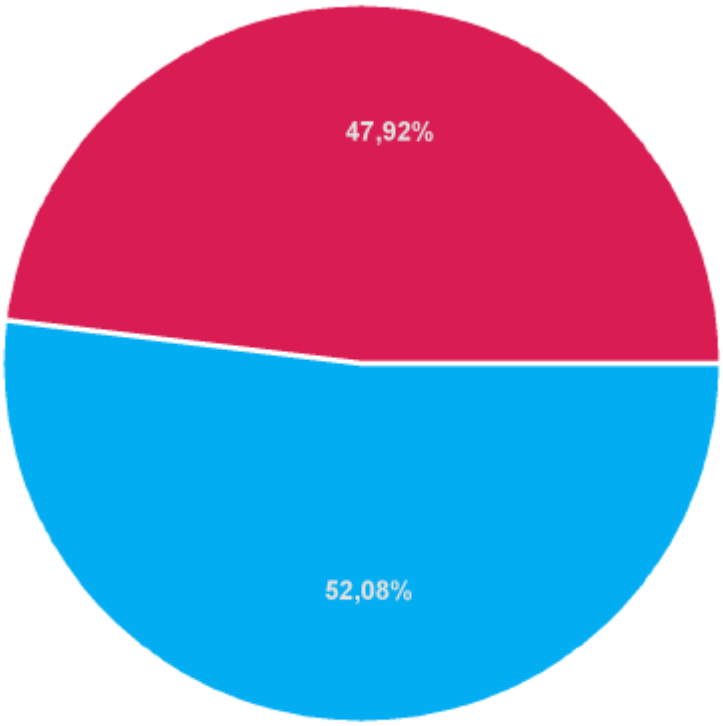
Сталкивались ли Вы когда-нибудь с экстремизмом в социальных сетях?



Да, сталкивался	75%	36
Нет, никогда не сталкивался	25%	12

Testograf.ru

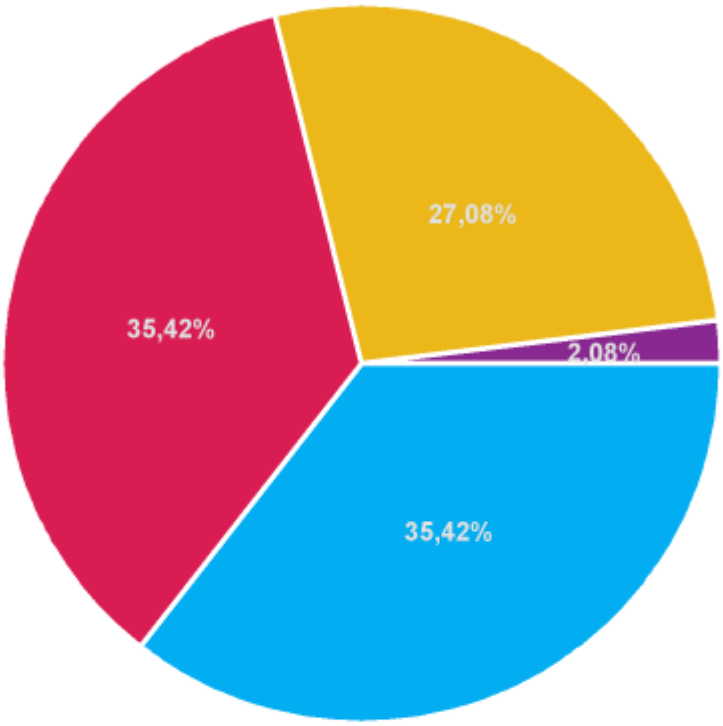
Знаете ли Вы, куда можно обратиться в случае обнаружения материалов экстремистской направленности в социальных сетях?



Нет, не знаю	52,08%	25
Да, знаю	47,92%	23

Testograf.ru

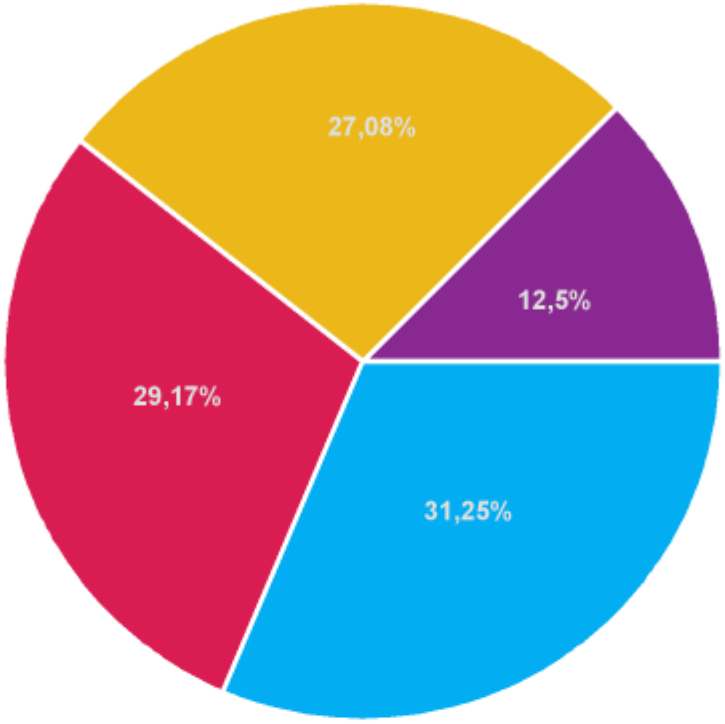
Что, по вашему мнению, является причиной активного использования социальных сетей в экстремистской деятельности?



Легкость и быстрота распространения информации в сети Интернет, т.к. социальные сети и форумы очень популярны среди молодежи	35,42%	17
Высокая анонимность общения (использование множества анонимизирующих программ, использование иностранных доменов и серверов).	35,42%	17
Минимальный контроль со стороны государственных структур	27,08%	13
Возможность быстрой ликвидации информационной базы.	2,08%	1

Testograf.ru

Для более эффективной борьбы с экстремизмом в социальных сетях необходимо...



Привлечь к работе по профилакте экстремистской деятельности наиболее популярных блогеров, готовых к диалогу и взаимодействию в противоборстве экстремизму.	31,25%	15
Создание при участии компаний, оказывающих услуги в сети Интернет, наблюдательных советов и «горячих линий», которые были бы наделены полномочиями оперативно удалять из глобальной сети материалы, содержащие экстремистскую направленность.	29,17%	14
Возложить персональную ответственность за пропаганду экстремизма создателей сетевых ресурсов.	27,08%	13
Задействовать потенциал социальных медиа, путем размещения материалов с антиэкстремистским контентом.	12,5%	6

Testograf.ru

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ.- 04 августа.- 2014.- № 31.Ст. 4398.

2. Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом (заключена в г. Шанхае 15.06.2001) // Собрание законодательства РФ. 2003. 13 октября. № 41. Ст. 3947.

3. Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ // Российская газета.- 18 августа.- 1995.- № 160.

4. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ.- 17 июня.- 1996.- № 25. Ст. 2954.

5. Кодекс Российской Федерации об административных правонарушениях: федеральный закон от 30.12.2001 № 195-ФЗ // Российская газета.- 31 декабря.- 2001.- № 256.

6. О противодействии экстремистской деятельности: Федеральный закон от 25.07.2002 № 114-ФЗ // Российская газета.- 30 июля.- 2002.- 138-139.

7. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Российская газета.- 29 июля.- 2006.- № 165.

8. О противодействии терроризму: федеральный закон от 06.03. 2006г. №35-ФЗ // Российская газета.- 2006г.- №48.

9. Вопросы Министерства юстиции Российской Федерации: Указ Президента РФ от 13.10.2004 № 1313 // Российская газета.- 19 октября.- 2004.- № 230.

10. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31.12.2015 // Собрание законодательства РФ.- 04 января.- 2016.- № 1 (часть II). Ст. 212.

11. Концепция противодействия терроризму в Российской Федерации: утверждена Президентом РФ от 05.10.2009 // Российская газета- 2009.- №198.

12. О судебной практике по уголовным делам о преступлениях экстремистской направленности : постановлению Пленума Верховного Суда РФ от 28.06.2011 N 11 // Российская газета. – 2011. – 4 июля (№11).

13. О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности: постановление Пленума Верховного суда РФ от 9.02.2012 г. №1 // Российская газета. – 17 февраля 2012 г. - № 35.

14. Авдеев, В.А., Авдеева, О.А. Механизм противодействия преступлениям террористического характера и экстремистской направленности в Российской Федерации // Юридический мир. 2014. № 12.

15. Агапов, П.А., Михайлов К.В. Уголовная ответственность за содействие террористической деятельности: тенденции современной уголовной политики. Саратов, 2007. 144 с.

16. Абалов И.Ю. Об использовании неформальными молодёжными объединениями сети интернет в целях осуществления экстремистской деятельности// Практические аспекты профилактики экстремизма и противодействия распространению его идеологии в молодежной среде : сборник научных трудов международной заочной научно-практической конференции. – Орехово-Зуево : Изд-во МГОГИ, 2013.

17. Алехин Е.В. Совершенствование законодательства как направление противодействия деятельности экстремистских сообществ // Российский следователь. 2011. N 3.

18. Белова, М.А., Рустамов, Н.Э. Правовые средства противодействия экстремизму по российскому праву // Административное и муниципальное право. 2015. № 1.

19. Борисов, С.В., Чугунов, А.А. Новеллы уголовного законодательства в сфере противодействия экстремизму: критический анализ // Современное право. 2015. № 4.

20. Бирюков, В.Г. Противодействие идеологии терроризма среди молодежи в сети Интернет // Ростовский научный журнал.- 2016.- №5.- С. 28-36.

21. Бахтеева, А. Р. Политический терроризм как социальное явление современности: дис. … канд. социолог. наук. М., 2010. С. 16.

22. Боташева, А.К. Политический терроризм: детерминация и формы проявления.: дис. … канд. полит. наук. Ставрополь, 2004. 183 с.

23. Бааль Н.Б. Политический экстремизм молодежи как острейшая проблема современной России // Российский следователь. 2007. N 7.

24. Берковец Л. Агрессия: причины, последствия, контроль. – М.: Олма-пресс, 2001. 235 с.

25. Воронцов, С.А. О необходимости совершенствования подходов к обеспечению национальной безопасности России в информационной сфере / С.А. Воронцов, А.Г. Штейнбух // Наука и образование: хозяйство и экономика; предпринимательство; право и управление.- 2015.- №9 (64).- С. 100-108.

26. Воронцов, С.А. Формирование угроз безопасности Российской Федерации как следствие кризиса культуры / С.А. Воронцов // Гуманитарные и социально-экономические науки.- 2013.- №5.- С. 111-115.

27. Васенина И. Ценностные ориентации студенческой молодежи и экстремизм // Высшее образование в России. 2007. № 11. - С. 116 - 119.

28. Григорьева, Л.В. О научном подходе к уголовно-правовой оценке действий экстремистской направленности // Современное право. 2015. № 7.

29. Гаухман, Л.Д. Уголовно-правовая борьба с терроризмом // Законность. - М., 2001, № 5. - С. 5-7.

30. Герасименко Т.В. Понятие и признаки терроризма // Закон и армия. Военно-правовая газета. - М.: Юрист, 2005, № 8. - С. 22-27.

31. Гладышев-Лядов Владимир Социальные сети как инструмент для пропаганды экстремизма // Обзор. НЦПТИ. 2013. №2. URL: http://cyberleninka.ru/article/n/sotsialnye-seti-kak-instrument-dlya-propagandy-ekstremizma (дата обращения: 14.12.2016).

32. Горбунов Ю.С. Терроризм и правовое регулирование противодействия ему: монография. – М.: Молодая гвардия, 2008. 460 с.

33. Дикаев С.У. Террор, терроризм и преступления террористического характера (криминологическое и уголовно-правовое исследование). – СПб.: Юридический центр «Пресс», 2006. 464 с.

34. Давыдов, В.О. Методика расследования экстремистских преступлений, совершенных в компьютерных сетях / под ред. А.Ю. Головина – М.: Юрлитинформ, 2014. 184 с.

35. Ещенко С.А. Меры противодействия проявлению экстремизма в России: постановка проблемы // Общество и право. – 2009. – № 2. – С. 11–15.

36. Зубок Ю.А., Чупров В.И. Молодежный экстремизм: сущность и особенности проявления // Социологические исследования. – 2008. – № 5. – С. 37– 47.

37. Залоило, М.В., Власова, Н.В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5.

38. Зинурова Р. И., Тузиков А. Р. Тренды молодежной политики за рубежом // Вестник Казанского технологического университета. 2012. Т. 15. № 10. С. 345-348.

39. Истомин А.Ф., Лопаткин Д.А. К вопросу об экстремизме // Современное право. Новое в российском законодательстве: обзоры, комментарии, практика 2005. №7.

40. Ильин, Е.П. Доклад первого заместителя руководителя аппарата НАК / Е.П. Ильин // Материалы III Всероссийской научно-практической конференции «Концепции противодействия терроризму в Российской Федерации».- Том. 1.- М., 2012.- С. 3-16.

41. История политических и правовых учений / под общ. ред. О. В. Мартышина. М.Норма, 2007. 890 с.

42. Капитонова Е.А., Романовский Г.Б. Современный терроризм: монография. – М.: Юрлитинформ, 2015. 216 с.

43. Кожушко, Е.П. Современный терроризм: анализ основных направлений. Минск: Харвест, 2000. 448 с.

44. Кубякин Е.О. Тенденции развития молодежного экстремизма в условиях прогресса информационно-компьютерных технологий // Вестник МГИМО. 2013. №3 (30). URL: http://cyberleninka.ru/article/n/tendentsii-razvitiya-molodezhnogo-ekstremizma-v-usloviyah-progressa-informatsionno-kompyuternyh-tehnologiy (дата обращения: 10.12.2016).

45. Кузьмин А.В. Социально-культурная профилактика экстремизма в молодежной среде: автореф. дис. … д-ра пед. наук. – Тамбов, 2012. 56 с.

46. Кузнецов, С.А., Оленников, С.М. Экспертные исследования по делам о признании информационных материалов экстремистскими: теоретические основания и методическое руководство (научно-практическое издание). М., 2014.

47. Котлярова В.В., Шубина М.М., Сысоева О.Н. Молодежный экстремизм в социальных сетях: специфика и теоретическое осмысление // URL: https://almavest.ru/ru/archive/1866/3469

48. Литвинова Т. Н. «Информационный джихад» в глобальной сети // Власть. 2010. №9.

49. Лелеков, В.А., Черных, А.А. О причинах преступлений экстремистской направленности в молодежной среде // Российский следователь. 2015. № 8.

50. Лунеев В.В. Курс мировой и российской криминологии в 2 т. Т. II. Особенная часть: учебник для вузов. – М.: Юрайт, 2013. 872 с.

51. Магомедтагиров А.М. Проблемы совершенствования практики применения законодательства для противодействия экстремизму // Законодательство и право. – 2010. – № 5. – С. 34–36.

52. Малышев В.В. Европейский опыт противодействия экстремизму // Правовая инициатива/ 2013. № 8. С. 2.

53. Макеева, И.С. Экстремизм как уголовно-правовая категория // Законодательство и экономика. 2014. № 6.

54. Михайлов, В. Процедура признания материалов экстремистскими требует коррекции // Административное право. 2015. № 1.

55. Морозова, Н.А. Проблемы привлечения к уголовной ответственности за экстремизм в информационной сети Интернет // Российский следователь. 2014. № 5.

56. Мохов В.В. Экстремизм в России: портрет явления // Мир безопасности. – 2008. – № 5. – С. 57–63.

57. Молодежный экстремизм в социальных сетях: специфика и теоретическое осмысление / В. В. Котлярова, М. М. Шубина, О. Н. Сысоева // Alma mater (Вестник высшей школы). - 2016. - № 5. - С. 95-99.

58. Нурлыбаева Г.К. Молодежный экстремизм и особенности противодействия со стороны полицейских служб Великобритании // Российский следователь. 2011. № 10.

59. Ожегов, С.И. Словарь русского языка. М., 1978. 846 с.

60. Оселков А.А., Психологические особенности влияния на студентов высших учебных заведений материалов экстремистской направленности: автореф. дис. канд. психол. наук. – Ростов-на-Дону, 2011. 26 с.

61. Перчаткина, С.А., Черемисинова, М.Е., Цирин, А.М., Цирина, М.А., Цомартова, Ф.В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2012. № 5.

62. Пугачев В.П. Соловьев А.И. Введение в политологию., , - М.: АСПЕКТ ПРЕСС, 2000.

63. Салахутдинов А. А. Социальные сети как информационный канал экстремистского материала // Молодой ученый. – 2014. - №17.

64. Сергун, Е.П. Экстремизм в российском уголовном праве: Автореферат дисс… канд. юрид. наук. Тамбов, 2009. 24 с.

65. Сальников Е.В. Экстремизм как медиакатегория. Монография. – Орел, ОрЮИ МВД России, 2012. 125 с.

66. Синцов Г.В. Информационная война с экстремизмом и терроризмом, - М., 2013.

67. Смагина, А.В., Сопун, Д.И. Причины распространения экстремизма в России // Российский следователь. 2012. № 8.

68. Степанов, В.В., Струков, А.В. Проблемы разрешения конкуренции составов преступлений экстремистской направленности // Вестник Пермского университета. Юридические науки. 2015. № 1.

69. Советский энциклопедический словарь / Науч.-ред. совет: А.Н. Прохоров (председатель). М.: Советская Энциклопедия, 1981. 1600 с.

70. Сивопляс, К.О. О противодействии идеологии терроризма в сети «Интернет» // Ростовский научный журнал.- 2016.- №7.- С. 5-12.

71. Смирнов В. А. Основы молодежной политики в сфере профилактики экстремизма // Вестник ЧГУ. Серия Философия. Социология. Культурология. 2008. № 14. Вып. 7. - С. 78-87.

72. Телешина, Н.Н. К вопросу о совершенствовании государственного контроля виртуального пространства // Информационное право. 2012. № 1.

73. Терешина Е. А. Противодействие молодежному экстремизму (на примере опыта Великобритании и США) // КПЖ. 2015. №1. URL: http://cyberleninka.ru/article/n/protivodeystvie-molodezhnomu-ekstremizmu-na-primere-opyta-velikobritanii-i-ssha (дата обращения: 10.12.2016).

74. Узденов, Р. М. Экстремизм: криминологические и уголовно-правовые проблемы противодействия : автореф. дис. ... канд. юрид. наук. М., 2008. 29 с.

75. Хлебушкин, А.Г. Экстремизм: уголовно-правовой и уголовно-политический анализ / Отв. ред. Н.А. Лопашенко. Саратов, 2007. 160 с.

76. Химилонова М.Т. Социальные сети: экстремизм и терроризм.- Владикавказ, 2016. 120 с.

77. Чурилов, С.А. Экспертная интернет-платформа как средство коллегиальной разработки методов информационного противодействия терроризму и экстремизму / С.А. Чурилов // Материалы II Всероссийской научно-практической конференции «Роль средств массовой информации и Интернета в предупреждении терроризма».- Том. 1.- М., 2013.- С. 87-92.

78. Шестаков, В. Террор – мировая война. М., 2003.

79. Щербинина, Ю.В. Вербальная агрессия. М., 2006.

80. Яковлев, А. Ю. И вновь о терроризме: еще одна попытка найти его дефиницию // Социально-гуманитарные знания. 2012. № 4. С. 118 – 119.

СВЕДЕНИЯ ОБ АВТОРАХ

Мазуров В.А. - доцент кафедры уголовного права и криминологии, кандидат юридических наук, доцент, руководитель НОЦ «Правовое обеспечение противодействия экстремизму и терроризму» Алтайского государственного университета.

Куликов Е.А. – доцент кафедры уголовного права и криминологии Алтайского государственного университета, кандидат юридических наук.

Суханова Е.П. – преподаватель кафедры уголовного права и криминологии Алтайского государственного университета.

Соколов А.С. – преподаватель кафедры уголовного процесса и криминалистики Алтайского государственного университета.

Косенко Д.В., Шалабод К.В. – студенты 4 курса юридического факультета Алтайского государственного университета.

Кузнецова Е.В., Яндиков М.С. – магистранты юридического факультета Алтайского государственного университета.

Бедарева А.А., Чудаева Д.К. - магистранты юридического факультета Алтайского государственного университета.

Кузеванова О.О. – магистрант юридического факультета Алтайского государственного университета.

Данилова Р.Р. - магистрант юридического факультета Алтайского государственного университета.

Ермакова А.С., Габриелян А.М. - магистранты юридического факультета Алтайского государственного университета.

Учебное издание

ПРЕСТУПНОСТЬ ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ В СФЕРЕ ВЫСОКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: ПРИЧИНЫ, УСЛОВИЯ, ПРОФИЛАКТИКА

Учебное пособие

Публикуется в авторской редакции
Дизайн обложки *Ю.В. Плетнева*

Издательская лицензия ЛР 020261 от 14.01.1997 г.

Подписано в печать 26.04.2018.
Формат 60х84 1/16. Усл.-печ. л. 9,07.
Тираж 100 экз. Заказ 170.

Типография Алтайского государственного университета

656099 Барнаул, ул. Димитрова, 66