DOI 10.54596/2309-6977-2022-4-121-128
УДК 327
МРНТИ 10.77.51

# КРИМИНАЛИЗАЦИЯ ИНТЕРНЕТ-ПРОСТРАНСТВА И ПРЕСТУПНАЯ ДЕЯТЕЛЬНОСТЬ ТЕРРОРИСТИЧЕСКИХ ГРУППИРОВОК В СОЦИАЛЬНЫХ СЕТЯХ

**Шут О.А.**[1,2]
*[1]ОмГУ им. Ф.М. Достоевского, Омск, Российская Федерация*
*[2]Северо-Казахстанский университет им. М. Козыбаева, Петропавловск, Республика Казахстан*
*[*]E-mail: shut_oxi@mail.ru*

**Аннотация**

Несмотря на все свои плюсы, интернет-пространство представляет огромную общественную опасность, так как, в частности, используется для совершения правонарушений. Правонарушения, совершенные в информационном пространстве, характеризуются высокой латентностью, так как у правоохранительных органов недостаточно возможностей для расследования и раскрытия данных преступлений, так как совершаться они могут на территории одного государства, при этом местонахождение правонарушителя может быть на территории совершенно другой страны или континента.

В данной статье рассматриваются криминализация информационного пространства и преступная деятельность экстремистских группировок в социальных сетях.

Актуальность данной статьи заключается в том, что в данной статье исследуются проблемы, появившиеся с распространением социальных сетей, и то, какую общественную опасность они представляют. Преступления, совершаемые посредством использования интернета, характеризуются высокой латентностью и представляют огромные проблемы для правоохранительных органов. Для борьбы с интернет-преступностью государствам необходимо усовершенствовать техническое обеспечение собственных правоохранительных органов.

**Ключевые слова**: интернет, экстремизм, терроризм, мошенничество, социальные сети, правонарушения, преступления.

# АҚПАРАТТЫҚ КЕҢІСТІКТІ КРИМИНАЛИЗАЦИЯЛАУ ЖӘНЕ ӘЛЕУМЕТТІК ЖЕЛІЛЕРДЕГІ ЭКСТРЕМИСТІК ТОПТАРДЫҢ ҚЫЛМЫСТЫҚ ӘРЕКЕТТЕРІ

**ШУТ О.А.**[1,2]
*[1]Ф.М. Достоевский атындағы ОМУ, Омбы, Ресей Федерациясы*
*[2]М. Қозыбаев атындағы Солтүстік Қазақстан университеті, Петропавл, Қазақстан Республикасы*
*[*]E-mail: shut_oxi@mail.ru*

**Аңдатпа**

Барлық артықшылықтарға қарамастан, ақпараттық кеңістік үлкен қоғамдық қауіп болып табылады, өйткені олар, атап айтқанда, құқық бұзушылық жасау үшін қолданылады. Ақпараттық кеңістікте жасалған құқық бұзушылықтар жоғары кідіріспен сипатталады, өйткені құқық қорғау органдарында бұл қылмыстарды тергеу және ашу үшін мүмкіндіктер жеткіліксіз, өйткені олар бір елдің аумағында жасалуы мүмкін, ал құқық бұзушының орналасқан жері мүлдем басқа елдің немесе континенттің аумағында болуы мүмкін.

Бұл мақалада ақпараттық кеңістікті криминализациялау және әлеуметтік желілердегі экстремистік топтардың қылмыстық әрекеттері қарастырылады.

Бұл мақаланың өзектілігі - бұл мақалада әлеуметтік желілердің таралуымен туындаған проблемалар және олар қандай әлеуметтік қауіп төндіретіні зерттеледі. Интернетті пайдалану арқылы жасалған қылмыстар жоғары кідіріспен сипатталады және құқық қорғау органдарына үлкен қиындықтар туғызады. Интернет-қылмыспен күресу үшін мемлекеттер өздерінің құқық қорғау органдарын техникалық қамтамасыз етуді жетілдіруі қажет.

**Түйінді сөздер**: интернет, экстремизм, терроризм, алаяқтық, әлеуметтік желілер, құқық бұзушылықтар, қылмыстар.

# CRIMINALIZATION OF THE INFORMATION SPACE AND CRIMINAL ACTIVITIES OF EXTREMIST GROUPS IN SOCIAL NETWORKS

**Shut O.A.** [1,2]

[1]*Dostoevsky Omsk State University, Omsk, Russia*

[2]*M. Kozybayev North Kazakhstan University, Petropavlovsk, Republic of Kazakhstan*

[*]*E-mail: shut_oxi@mail.ru*

**Abstract**

Despite all its advantages, the information space is a huge public danger, since, in particular, it is used to commit offenses. Offenses committed in the information space are characterized by high latency, since law enforcement agencies do not have enough opportunities to investigate and disclose these crimes, since they can be committed on the territory of one country, while the location of the offender may be on the territory of a completely different country or continent.

This article discusses the criminalization of the information space and the criminal activity of extremist groups in social networks.

The relevance of this article lies in the fact that this article examines the problems that have appeared with the spread of social networks, and what kind of public danger they pose. Crimes committed through the use of the Internet are characterized by high latency and pose huge problems for law enforcement agencies. To combat Internet crime, States need to improve the technical support of their own law enforcement agencies.

**Key words:** internet, extremism, terrorism, fraud, social networks, offenses, crimes.

## Введение

Распространение интернета и его огромные масштабы произвели резолюцию в коммуникационных технологиях. Резко изменились и способы обмена информацией между людьми, особенно после появления электронной почты и файлообменников, а позже и различных социальных сетей.

Нет никаких сомнений в том, что появление интернета и развитие компьютерных технологий дало новый толчок к развитию современных технологий, а также к заметному улучшению качеству жизни людей на земле. Получив повсеместное распространение, глобальная сеть интернет позволила всем людям на планете безграничный доступ к информации и возможность ею обмениваться. Люди сразу оценили возможность интернета и его потенциал для общения между собой. Таким образом, практически сразу же начали появляться социальные сети.

Появление социальных сетей полностью изменило отношение людей к информации. Всемирная сеть дала возможность всему миру обмениваться разными мнениями без взаимодействия с традиционными СМИ вроде газет, радио и телевизора, что является более демократическим, так как пользователи получили возможность распространять свое мнение без цензуры в СМИ. На данный момент интернет стал неотъемлемой частью наших жизней, став важной частью государственных учреждений. Посредством интернета совершаются банковские операции, осуществляется документооборот в государственных органах, граждане получают доступ к различным базам данных.

Однако несмотря на все эти плюсы, интернет давно стал площадкой для совершения преступлений. Мошенничество, интернет буллинг и угрозы, продажа оружия и наркотиков – вот одни из множества преступлений, совершаемых в социальных сетях [1].

Киберпреступностью считается любая преступная деятельность, совершенная посредством использования компьютеров, компьютерных сетей и других информационно-коммуникационных технологий. В основном они совершаются с корыстным мотивом, с целью извлечения выгоды. Но иногда бывают случаи совершения киберпреступлений против компьютеров, ради вывода из строя устройств. Часто преступники используют интернет ради распространения вредоносных программ, вирусов, майнеров, шпионских программ, компьютерных червей, а также незаконной информации. Существует много различных видов киберпреступлений. Среди них можно отметить атаки персональных компьютеров, создание и распространение программ-вымогателей, интернет-мошенничество, кража и распространение персональной информации.

Актуальность темы данной статьи заключается в том, что в нынешнее время, в связи с глобальной пандемией и переводом большинства работников на дистанционную работу и вследствие зависимости их от интернета, уровень киберпреступности возрос в разы. Под угрозой оказались частная и корпоративная информация, которая хранится в базах данных, доступ к которым осуществляется при помощи интернета. Например, статистика отмечает рост мошеннических действий, совершенных посредством глобальной сети интернет в последние годы. В связи с этим возрастает необходимость более глубокого изучения данной темы для того, чтобы понять каким образом необходимо бороться с растущей интернет-преступностью.

Криминализация интернет-пространства началась чуть ли ни с самого его основания, а правоохранительных органам осталось только поспевать за преступниками, для их вычисления и поимки. Однако, как и не стоят на месте информационно-коммуникационные технологии, таким же темпом развиваются преступления в социальных сетях и, к сожалению, на данный момент правоохранительные органы недостаточно оснащены всей необходимой технической базой.

Социальные сети используются не только ради совершения преступлений против собственности. К сожалению, в последние годы растет число террористических преступлений в социальных сетях. Террористические группы используют рост популярности социальных сетей и возрастание их пользователей в собственных целях. Социальные сети становятся удобной площадкой для распространения собственных идей и вербовки новых членов. Таким образом, террористы-одиночники, проникшись идеями, пропагандируемые в социальных сетях, совершают террористические акты.

Повсеместное распространение интернета дало возможность террористическим группам вербовать людей по всему миру используя различные социальные сети, такие как Facebook и Twitter и т.д. Обращаясь к разочаровавшимся в своей жизни, в обществе, в системе людям, они пытаются внушить им террористическую идеологию и заставить чувствовать их обязанными совершать террористические акты. Данные лица находятся под сильным влиянием террористов и в конечном итоге совершают необдуманные поступки, что и является целью террористических группировок.

## Методы исследования

В нашем веке цифровых технологий, когда интернет стал неотъемлемой частью жизни большинства людей на планете, превратившись в средство обмена информацией,

становится очевидным вопрос о необходимости сохранения конфиденциальности, а также целостности и защиты всей той информации, которой люди обмениваются.

Изучение криминализации информационного пространства – это важный фактор в осмыслении и понятии преступности и его влиянии на нынешнее общество. Для более точного изучения криминализации информационного пространства были использованы некоторые общенаучные методы, как анализ и обобщение литературы.

Также в данной статье исследуется использование террористами социальных сетей, а также совершен анализ социальных сетей, как площадки для вербовки новых членов террористических группировок.

Правонарушителей привлекает то, что посредством информационных технологий можно завладеть банковскими счетами или любой конфиденциальной информацией, а также шантажировать людей, не выходя из дома и, скорее всего они останутся безнаказанными [2].

В основном киберпреступления связаны с перехватом и распространением конфиденциальной информации, что приводит к таким преступлениям как мошенничество с банковскими счетами, кибервымогательство и компьютерный шпионаж.

Большинство из этих преступлений так и остаются нераскрытыми, а правонарушители остаются на свободе, продолжая нарушать закон. Это происходит по той причине, что преступления чаще всего совершаются за пределами юрисдикции органов внутренних дел конкретного государства, так как правонарушитель находится в другой стране или, что нередко, на другом континенте. Также часто используются анонимные компьютерные сети, с помощью которых невозможно отследить, лицо совершившее преступление. Данные сети полностью конфиденциальны. Торговля запрещенными веществами может проходить под видом обычного интернет-магазина, которых в сети огромное количество, а уследить за всеми невозможно. Все вышеперечисленное усложняет работу правоохранительным органам и не дает им раскрыть данные категории преступлений [3].

Конечно, правоохранительные органы блокируют и пресекают все обнаруженные незаконные действия в сети, однако на их месте тут же совершают новые, но куда более совершенные и недоступные для распознавания правоохранительными органами.

Куда опаснее совершаемые террористические преступления в социальных сетях. Некоторое время назад террористы не использовали социальные сети, а обходились засекреченными паролями форумами для обмена информацией и распространения пропаганды. Однако стремясь адаптироваться к современным реалиям, когда большинство людей используют социальные сети, террористические группировки начали использовать социальные сети для охвата более широкой аудитории. Также, социальные сети являются бесплатной площадкой для загрузки анонимного контента, автор которого может закрыть к нему публичный доступ. Таким образом, террористы тщательно проверяют всех лиц, интересующихся их организацией, чтобы не допустить проникновения сотрудников полиции.

## Результаты исследования

Появление интернета не только предоставило правонарушителям совершенно новые способы совершения отдельных видов преступлений, например, таких как мошенничество, вымогательство, кражи, но и предоставило возможность совершать

новые преступления, первые в своем роде и не предусмотренные законодательством стран мира.

Многие люди, особенно старшего поколения, совершенно безграмотны в вопросе сохранения и защиты своих данных и не используют меры предосторожности при использовании глобальной сети интернет. Они не используют антивирусы и таким образом ставят под угрозу свое пребывание в сети интернет, даря возможность правонарушителям завладеть их персональными данными, заразить свой персональный компьютер вирусами, различными программами фишерами, майнерами и т.д. Происходит это потому, так как большинство пользователей сети недооценивают свою возможность стать жертвами преступлений, просто пребывая, например, в социальной сети. Некоторые люди и не догадываются об онлайн-угрозах, которые могут нанести им существенный вред.

В странах СНГ многие жертвы сталкиваются с отсутствием средств правовой защиты на местном уровне. Преступления совершенные посредством использования сети интернет, часто остаются нераскрытыми, а жертвы не получают должной компенсации. Органы внутренних дел не имеют технических возможностей для расследования киберпреступлений. Обычно внимание уделяется особо опасным преступлениям, таким как терроризм и совершенным на сексуальной почве, педофилии.

Еще одной большой проблемой является транснациональный характер совершения киберпреступлений. В данном случае жертва и преступник могут находиться в разных странах, что значительно затрудняет работу правоохранительных органов. Также в данном случае они подсудны различным законодательствам, и то деяние, которое в одном государстве считается преступлением, в другом может и не влечь за собой никаких последствий.

Часто преступники используют интернет ради распространения вредоносных программ, вирусов, майнеров, шпионских программ, компьютерных червей, а также незаконной информации.

Существует много различных видов киберпреступлений. Среди них можно отметить атаки персональных компьютеров, создание и распространение программ-вымогателей, интернет-мошенничество, кража и распространение персональной информации. В основном они совершаются с корыстным мотивом, с целью извлечения выгоды.

Интернет-мошенничество – это вид мошенничества, совершаемое с помощью информационно-коммуникационных технологий. Интернет-мошенничество включает в себя фишинг, кражу личных данных и распространение программ вымогателей. По составу данное правонарушение практически не отличается от обычного мошенничества с небольшим дополнением. С объективной стороны интернет-мошенничество можно определить, как хищение чужого имущества или приобретения права на чужое имущество путем обмана или злоупотребления доверием с использованием информационно-коммуникационных технологий.

Программой вымогателем называется программное обеспечение, влияющее на нормальную работу компьютера и требующее оплаты для возвращения его в первоначальное состояние. Правонарушители, используя данную программу требуют от жертвы выкуп угрожая публикацией каких-либо личных данных жертвы или полной блокировкой к ним. Продвинутые программы обычно зашифровывают файлы владельца компьютера, расшифровать которые простому пользователю компьютера не представляется возможным ввиду отсутствия знаний в данной области.

Правонарушители требуют выкуп в криптовалюте, что не позволит вычислить их местонахождение правоохранительными органами. Программы вымогатели обычно попадают на компьютер под видом обычных файлов, используется принцип троянского коня.

Фишингом называется интернет-мошенничество, совершаемое ради кражи персональных данных. Совершается оно посредством рассылки электронных писем, содержащих ссылки на сайты, через которые может быть установлена похищающая личные данные злонамеренная программа на компьютер.

Программы вымогатели шантажируют владельцев компьютеров публикацией конфиденциальной информации, в некоторых случаях могут блокировать доступ к важным файлам или даже к самой системе, препятствуя нормальной работе компьютера. Преступники требуют выкуп за обещание не публиковать личную информацию или для возвращения прежней работы системы. Для выкупа же используются криптовалюты, что затрудняет дальнейшее отслеживание денежных переводов.

Одной из глобальных проблем являются незаконные террористические сообщества в социальных сетях. В основном их целевой аудиторией являются подростки, так как их неустойчивая психика позволяет преступниками манипулировать ими и призывать их к насилию. В таких пабликах публикуется специально подготовленные материалы, способные вызвать у подростков чувство агрессии к определенным социальным феноменам.

Состав преступления также практически не отличается от других преступлений против общественной безопасности и общественного порядка. Общественной опасностью данных действий будет считаться представление угрозы для безопасности общества, угрозы совершения актов терроризма, опасность гибели людей, угроза причинения имущественного ущерба либо наступления иных общественно опасных последствий. Объективная сторона характеризуется действиями, заключающимися в пропаганде терроризма или призывах к совершению акта терроризма, а также в распространении материалов террористического содержания.

Террористические группировки внушают доверчивым людям ложную информацию, таким образам привлекая все больше и больше людей для совершения различного рода террористических актов. Вербовка включает в себя распространение материалов экстремистского характера, видеозаписи совершенных террористических актов и с выступлениями лидеров террористических группировок.

В целях получения денежных средств террористы создают веб-сайты, различные чаты для распространения информации, а также занимаются массовой рассылкой. Нередки и случаи мошенничества, когда преступники под видом интернет-магазинов обманом заполучают деньги граждан.

Большой проблемой является то, что террористические группировки используют интернет в качестве площадки для финансирования собственной деятельности. Деньги могут приходить на их счет как прямыми платежами, так и пожертвованиями для вымышленных благотворительных организаций. Однако они не останавливаются на вымышленных благотворительных организациях, существовали случаи создания подставных благотворительных фондов террористами, среди которых можно назвать Benevolence International Foundation, Holy Land Foundation for Relief and Development, Global Relief Foundation.

Но самой главной проблемой, пожалуй, можно назвать использование интернета для тренировки членов террористических группировок. В сети распространяются

различные материалы, пособия и фильмы, в которых содержится представляющая огромную опасность информация. Публикуются материалы о создании взрывчаток, огнестрельного оружия, о планировании террористических актов [4].

Из-за того, что террористы находятся на большом расстоянии друг-от друга, многие группировки для коммуникации используют интернет-форумы, сайты и социальные сети. Здесь у них существуют специальные шифр и команды, понятные им самим, что усложняет работу полиции, так как данные форумы могут быть замаскированы под совершенно безвредные сайты.

Согласно данным ООН именно благодаря интернету ИГИЛ завербовали на свою сторону множество людей. Они привлекают на свою сторону людей с религиозными, расовыми и национальными предубеждениями, так как ими проще всего манипулировать. Поиском данных лиц они занимаются все на тех же форумах и сайтах, посвященных различного рода дискриминациям. ИГИЛ и иные группировки используют интернет в первую очередь как способ вещания. Интернет отлично подходит для пропаганды, проектировки общественного мнения. Чтобы придать легитимность своим действиям в глазах читающих, они выкладывают в сеть статьи о недовольстве действующей властью, о злоупотреблении ею властью и выставляют себя в качестве борцов с несправедливостью [5].

Глобальную сеть интернет можно сравнить с инструментом, который может быть использован как в законных, так и в незаконных целях. Однако проблема состоит в том, что, используясь для совершения преступлений, интернет представляет большую общественную опасность. Преступления становится легче совершать, и они часто остаются безнаказанными.

На данный момент решить данную проблему невозможно, даже использование самых радикальных мер не является решением. В истории существовали прецеденты блокировки анонимных компьютерных сетей правительствами различных государств, но данные действия подверглись критике со стороны многих правозащитников. По их мнению, запрещая анонимайзеры, нарушаются права человека на свободу слова и неприкосновенность частной жизни.

Единственным решением видится развитие информационно-коммуникативных технологий правоохранительных органов, для того чтобы вести борьбу с киберпреступниками на равных условиях. Также государствам необходимо содействовать друг-другу при уголовном преследовании киберпреступников и разрабатывать договоренности относительно межгосударственного сотрудничества.

В качестве научной новизны данной работы можно выделить то, что развитие технологий приносит не только благо нашему обществу, но и влечет за собой некоторые проблемы. Развитие интернета привело к тому, что стали появляться новые формы преступлений. Правоохранительные органы государств не всегда поспевают за технологическим прогрессом, а, следовательно, за преступниками. Государствам необходимо постоянно обновлять техническое обеспечение своих правоохранительных органов, а также модернизировать собственное уголовное законодательство.

## Заключение

Таким образом, на данный момент очень сложно измерить рост совершаемых киберпреступлений, в связи с постоянно растущими глобальными возможностями сети Интернет, а также свободным доступом к нему и растущими возможностями людей приобретения персональных компьютеров. Воздействие, оказанное интернетом на мир,

можно считать огромным, он повлиял практически на все сферы жизни людей. В развитых странах невозможно приставить себе и дня без использования интернета. Посредством глобальной сети проводят банковские транзакции, государственные органы получают доступ ко всем своим базам данных, люди совершают покупки в интернет-магазинах. Распространение интернета и его огромные масштабы привели к росту киберпреступлений во всем мире.

Интернет-пространство чуть ли не с самого основания стало удобной площадкой для совершения киберпреступлений. Мошенничество, кража персональной информации, интернет-угрозы, продажа запрещенных веществ – это только верхушка айсберга. Интернет для пропаганды также используют различные террористические группировки, что представляет огромную угрозу для всего мира. К сожалению, правоохранительные органы очень редко раскрывают данную категорию преступлений, ввиду высокого уровня их латентности. Именно поэтому государствам необходимо сотрудничать друг с другом для эффективной борьбы с киберпреступлениями.

Повсеместное распространение интернета дало возможность террористическим группам вербовать людей по всему миру используя различные социальные сети. Обращаясь к разочаровавшимся в своей жизни, в обществе, в системе людям, они пытаются внушить им террористическую идеологию и заставить чувствовать их обязанными совершать террористические акты. Социальные сети становятся удобной площадкой для распространения собственных идей и вербовки новых членов. Таким образом, террористы-одиночники, проникшись идеями, пропагандируемые в социальных сетях, совершают террористические акты.

**Литература:**

1. Номоконов В.А. Киберпреступность, как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология. Вчера. Сегодня. Завтра. - 2012. - №1 (24). - С. 47.
2. Даркнет: темная сторона Интернета // Официальный интернет-портал Парламентская газета. - URL: https://www.pnp.ru/politics/darknettemnaya-storona-interneta.html (дата обращения: 20.09.2021).
3. Нишанов Р.Ш. К вопросу о возможной криминализации распространения Tor-технологий - Актуальные проблемы взаимосвязи уголовного права и процесса - Сборник материалов Всероссийской научно-практической конференции с международным участием. - 2016 - С. 269-272.
4. Как используют сеть Интернет экстремистские и террористические организации? [Электронный ресурс]. URL: https://internetpolicy.kg/literacymodule/course_2/module2/glava2_2.html.
5. Террористы осваивают киберпространство и вербуют «одиночек» [Электронный ресурс]. URL: https://news.un.org/ru/story/2021/01/1394092.

**References:**

1. Nomokonov V.A. Cybercrime as a new criminal threat / V.A. Nomokonov, T.L. Tropina // Criminology. Yesterday. Today. Tomorrow. - 2012. - №1 (24). - P. 47.
2. Darknet: the dark side of the Internet // The official Internet portal Parliamentary Newspaper. - URL: https://www.pnp.ru/politics/darknettemnaya-storona-interneta.html (accessed: 09/20/2021).
3. Nishanov R.Sh. On the issue of possible criminalization of the spread of Tog technologies - Actual problems of the relationship between criminal law and process - Collection of materials of the All-Russian Scientific and Practical Conference with international participation. - 2016 - pp. 269-272.
4. How do extremist and terrorist organizations use the Internet? [electronic resource]. URL: https://internetpolicy.kg/literacymodule/course_2/module2/glava2_2.html.
5. Terrorists master cyberspace and recruit "singles" [Electronic resource]. URL: https://news.un.org/ru/story/2021/01/1394092.