УДК 004

Колгинова Ксения Георгиевна
Студент, юридический институт
Специальность: 40.03.01 Юриспруденция
“Белгородский государственный Национальный исследовательский университет”
РФ, г. Белгород
Научный руководитель: Бородаенко Наталья Васильевна,
старший преподаватель НИУ «БелГУ»,
Россия, г. Белгород

СОВРЕМЕННЫЕ УГРОЗЫ И ВЫЗОВЫ ИНФОРМАЦИОННОМУ ОБЩЕСТВУ

Аннотация: *Информация в настоящее время стала одним из ключевых ресурсов политического и социального развития общества. Однако ко всему этому информатизация привела к возникновению новых угроз, таких как информационные войны, информационный терроризм и кибератаки. Данные угрозы всегда направленны на психику и эмоциональное состояние людей. Инфотерроризм – это, прежде всего, распространение заведомо ложных сведений с целью подавления здравомыслия в обществе и лишения человека здраво рассуждать.*

Ключевые слова: *информационное общество, информационный терроризм, информация, кибертерроризм, интернет.*

Annotation: *Information has now become one of the key resources for the political and social development of society. However, in addition to all this, informatization has led to the emergence of new threats, such as information wars, information terrorism and cyber attacks. These threats are always aimed at the psyche and emotional state of people. Infoterrorism is, first of all, the dissemination*

of deliberately false information in order to suppress sanity in society and deprive a person of sound reasoning.

Keywords: *information society, information terrorism, information, cyberterrorism, Internet.*

В современном мире информация играет ключевую роль в социальном и политическом развитии. Она стала главным ресурсом благодаря быстрой циркуляции и передаче через средства массовой информации, особенно интернет. Таким образом, создалась новая среда обитания человека, где находятся как люди, так и механизмы воздействия на их сознание. Отличительной особенностью этой сферы является ее постоянное развитие и изменение, что требует от нас быть в курсе последних событий и новостей. Важно уметь фильтровать информацию и выбирать только достоверную и значимую для нас. В таком контексте развития актуальное значение, как угрозы, приобретают понятия “инфотерроризм” и “кибертерроризм”.

Инфотерроризм – это, прежде всего, прямое влияние на психику человека и его сознание, дабы сформировать у него у него нужные суждения, направляющие определенным образом поведение человека. Данный вид терроризма представляет собой предельно опасное асоциальное явление. Как и любой вид преступной деятельности, инфотерроризм имеет свою собственную цель – расшатывание конституционного строя. На мой взгляд, он наиболее распространен в более неспокойное, военное время. Как высказался однажды российский журналист В.Р. Соловьев: “…давно надо понять, что в современном мире информационные средства являются средством ведения войны. И информационные бомбы работают не менее эффективно, чем всякие прочие виды оружия...” В мирное время главные инициаторы инфотеррора на территории нашей державы – это:

- Иностранные спецслужбы и прочие иностранные организации
- Зарубежные и российские оппозиционные СМИ

- Экстремисткие группы

Инфотерроризм опирается на официальные СМИ, а также на распространение всякого рода слухов. В целом, слухи играют важную роль в вопросах терроризма. Они, как правило, усиливают чувство страха и ужаса, создаваемое и такое нужное террористам.

Инфотеррор применяется в определенных сферах, в которых могут быть предпосылки для идеологического либо же экономического противостояния. Можно отнести следующее к механизмам инфотеррора:

- Формирование общественного мнения благодаря СМИ
- Распространение агитационных материалов

Инфотерроризм, хоть и не предполагает физического насилия, но может привести к более опасным последствиям. Современное общество все больше ориентируется на информацию, поэтому контроль над ее распространением может стать мощным инструментом воздействия на поведение людей. Ведь для того, чтобы изменить мнение и действия общества, необходимо управлять информационными потоками, которые циркулируют в социальных сетях и СМИ.

Кибертерроризм представляет собой использование интернета для совершения насильственных действий, приводящих к гибели людей. Его цель – это достижение политических либо же идеологических выгод посредством угроз или запугивания. В общем и целом, кибертерроризм можно считать и как инструмент, и как составляющую инфотеррора. В наше время террористы обладают неограниченными возможностями, которые предоставляет интернет. Они имеют свободный доступ в сеть, могут не беспокоиться о цензуре и, самое главное, остаются анонимными. В настоящее время террористы используют интернет в основном для пропаганды своей деятельности. Например, в 2011 году известное террористическое объединение "Аль-Каида" запустило онлайн-журнал "Вдохновение" на

английском языке. В этом издании призывалось к участию единомышленников в достижении общей цели - просвещения каждого. В статьях, комментариях и отзывах участников журнала пропагандировалась идея о привнесении своего вклада в борьбу за общее благо.[1]

Специалисты в области права и государственные чиновники считают, что кибертерроризм является одной из самых серьезных угроз, сравнимой с оружием массового поражения. Особенно это актуально для энергетических систем, которые являются наиболее уязвимыми для кибератак, подчеркивает МЧС России. В настоящее время в России активно внедряются автоматизация и информатизация в разных отраслях промышленности, что делает борьбу с кибертерроризмом приоритетной задачей государства. Необходимость защиты от киберугроз стала существенной, и эксперты в области информационной безопасности уделяют этому вопросу все большее внимание. [2]

В современном мире информационная сфера играет ключевую роль в экономике, культуре и политике. Однако, она также является наиболее уязвимой к новым и изощренным формам преступности. Быстрый прогресс телекоммуникационных и глобальных сетей создаёт условия для компьютерных преступлений, которые становятся все более распространенными. Широкое распространение интернета, ранее доступного только узкому кругу пользователей, увеличило в разы потенциал компьютерных преступлений.

По последним отчетам ITU и GSMA Intelligence, количество пользователей Интернета на январь 2023 года достигло 5.16 миллиардов человек, что означает, что более 64% населения земного шара имеют доступ к сети. За прошедший год количество интернет-пользователей выросло на 1.9%, а онлайн-аудитория увеличилась на 98 миллионов человек. Однако, рост за год оказался несколько медленнее, чем в 2010 году, составив менее 2%. Таким

образом, можно сделать вывод о стабилизации рынка интернет-пользователей. [3]

В последние годы международное сообщество уделяет особое внимание проблеме борьбы с киберпреступностью. В связи с этим было разработано несколько международно-правовых документов, например, Будапештская конвенция по борьбе с киберпреступностью от 23 ноября 2001 г. [4] Этот документ позволяет регулировать действия различных государств по борьбе с преступностью в интернете. Однако российскую сторону не удовлетворила возможность вмешательства иностранных спецслужб в работу компьютерных сетей без официального уведомления, так как это может поставить под угрозу её безопасность и суверенитет.

Вскоре после распада СССР, Россия активно включилась в процессы информатизации и глобализации. В 1994 году был зарегистрирован домен ".ru", открывая доступ к интернету для многих пользователей. Однако, это привело к появлению первых хакеров и осознанию Россией необходимости решения проблем, связанных с безопасностью в интернете. Такое распространение интернета представляло опасность для российского общества, поскольку без контроля правительства он позволял свободное общение с иностранными сообществами и влияние на их политические взгляды.[5]

В связи с этим, в 1998 году Россия приняла инициативу по введению мер по информационной безопасности, которые были обсуждены на многосторонней основе. Эти меры были приняты для защиты общества и государства от потенциальных угроз в интернете. Сегодня интернет является неотъемлемой частью нашей жизни, и его безопасность и защита остаются приоритетными задачами.

В 2006 году были приняты два важных федеральных закона в России: "Об информации, информационных технологиях и о защите информации" и "О персональных данных". Они стали важным шагом в обеспечении

национальной безопасности в информационной сфере. В последующие годы были разработаны другие ключевые документы, отражающие концепцию нашего информационного пространства. Например, "Доктрина информационной безопасности" от 2016 года и Федеральный Закон "О критической информационной инфраструктуре" от 2017 года. Мы видим информационное пространство как пространство безопасности, равенства и суверенитета. Никакая страна в мире не может установить законы в одностороннем формате. Попытка доминирования в информационной среде является одной из значительных угроз, включая преступную деятельность в киберпространстве.[6]

В России с каждым годом растет количество киберпреступлений. В конце января 2023 г. Министерство внутренних дел РФ опубликовало статистику преступности в стране. В частности, цифры по незаконной деятельности, связанной с информационными технологиями, вошли в неё. На официальном сайте МВД было опубликовано сообщение, в котором отмечается, что показатели киберпреступности остаются стабильными. [7] Однако, следует обратить внимание на то, что каждое четвертое преступление совершается при использовании высоких технологий. Это подчеркивает важность защиты персональных данных и информации в интернете. Оставайтесь бдительными и не рискуйте своей безопасностью в виртуальном мире. В 2022 г. преступления, совершенные благодаря информационно-коммуникационным технологиям, пошли на убыль впервые с 2017 г. (за весь 2017 г. в стране было зафиксировано 90587 киберпреступлений). Такую позитивную динамику эксперты связывают, во-первых, с повышенной осведомленностью людей о злоумышленниках, и во-вторых, с спадом активности преступников на фоне Специальной Военной Операции России на Украине.

В 2001 году Межведомственная комиссия Совета Безопасности Российской Федерации по информационной безопасности утвердила

"Основные направления нормативного правового обеспечения информационной безопасности Российской Федерации" решением № 5.4 от 27.11.2001. Для усовершенствования правовой базы в области информационной безопасности разрабатываются законопроекты, такие как "О персональных данных", "О праве на информацию", "О коммерческой тайне", "О неприкосновенности частной жизни, о личной и семейной тайне", "О защите нравственности", "О служебной тайне" и "О национальной безопасности". Это необходимо для повышения эффективности защиты информации и обеспечения безопасности в Российской Федерации. [8]

В наше время борьба с преступностью, в том числе кибертерроризмом, стала одной из главных задач информационного общества. Ее сложность заключается в том, что преступники умело маскируют свои действия и масштабы преступлений могут быть огромными. Особенно это актуально в случаях, когда данные из информационных сетей постоянно меняются. Для эффективного борьбы с преступностью и сбора доказательств в режиме реального времени необходимо использовать адаптивные меры обеспечения возможности электронного сбора данных. Какие именно меры могут быть использованы, описано в Рекомендациях Совета Европы № R(95)13, которые регулируют проблемы уголовно-процессуального права, связанные с информационными технологиями. [8]

Все вышеизложенное показывает, что никакая страна в мире не может одна бороться с кибертерроризмом и другими угрозами для информационного общества. Для достижения максимальной эффективности необходимо согласованное международное сотрудничество. Только тогда можно достичь значительных результатов в этой области.

Литература:

1. “Аль-Каида” и ее журнал “Вдохновение” [Электронный ресурс]. URL: https://inosmi.ru/20110405/168092673.html (дата обращения: 25.04.2023)
2. МЧС считает кибертерроризм одним из ключевых рисков. [Электронный ресурс]. URL: http:// i-business.ru/blogs/16367 (дата обращения: 25.04.2023)
3. Вся статистика интернета и соцсетей на 2023 год – цифры и тренды из отчета Global Digital 2023 [Электронный ресурс]. URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/ (дата обращения: 27.04.2023)
4. Российский дипломат назвал будапештскую конференцию по киберпреступлениям устаревшей. Сайт ТАСС [Электронный ресурс]. URL: https://tass.ru/politika/4782506 (дата обращения: 25.04.2023)
5. Рунет – история появления интернета в России [Электронный ресурс]. URL: https://ren.tv/longread/960499-kak-sozdavalsia-i-razvivalsia-runet (дата обращения: 27.04.2023)
6. Внутренние вызовы и угрозы информационной безопасности Российской Федерации [Электронный ресурс]. URL: https://www.elibrary.ru/item.asp?id=35203935 (дата обращения: 30.04.2023)
7. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2022 года [Электронный ресурс]. URL: https://мвд.рф/reports/item/35396677/?year=2022&month=12&day=22 (дата обращения: 25.04.2023)
8. Классификация информационных угроз современному обществу [Электронный ресурс]. URL: https://www.elibrary.ru/item.asp?id=12786388 (дата обращения: 30.04.2023)
9. Алексеева И.Ю. Информационные вызовы национальной и международной безопасности. — М.: ПИР-Центр, 2001.

10. Газизов Р.Р. Информационный терроризм. Материалы международной научно-практической конференции 16—17 октября 2003 года. Часть I. — Уфа: РИО БашГУ, 2003.
11. Гриняев С.Н. Информационный терроризм: предпосылки и возможные последствия // Журнал теории и практики Евразийства.
12. Кулибаба А.Н. Информационный терроризм. [Электронный ресурс]. URL: http://www.inauka.ru (дата обращения: 25.04.2023)
13. Касьяненко, М.А. Правовые проблемы при использовании Интернета в транснациональном терроризме / М. А. Касьяненко // Информационное право. – 2012. – № 1. − С. 21–25.
14. Капитонова Е.А. Особенности кибертерроризма как новой разновидности террористического акта. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/osobennosti-kiberterrorizma-kak-novoy-raznovidnosti-terroristicheskogo-akta (дата обращения: 25.04.2023)