ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

4. Фонарев А.В. Особенности и основные типы политического лидерства // Вестник БГУ. 2014. №2. URL: https://cyberleninka.ru/article/n/osobennosti-i-osnovnye-tipy-politicheskogo-liderstva (дата обращения: 07.04.2024).
5. Лэй Э. Харизма. Искусство производить сильное и незабываемое впечатление: пер с англ. – М. : Протекст, 2010. – 277 с
6. Гарет Джонс, Роб Гоффи. Четыре свойства харизматичных лидеров. 03.12.2019 //https://big-i.ru/150ideas /leader_ rules /817769/
7. Харизматический лидер. 02.04.2024 // http://hr-ru.com/2010/08/xarizma-lidera-v-biznese/
8. Шкурко О. В. Харизматическое лидерство и возможность его развития у современных руководителей // Вестник ОмГУ. Серия: Экономика. 2013. №3. URL: https://cyberleninka.ru/article/n/harizmaticheskoe-liderstvo-i-vozmozhnost-ego-razvitiya-u-sovremennyh-rukovoditeley (дата обращения: 08.04.2024).

УДК 341

КИБЕРТЕРРОРИЗМ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Оралов Асылхан Раздыкович
sajasata@mail.ru
Докторант факультета международных отношений
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан, [2]
Аубакирова Динара Ниязбековна
a_d_n_94@mail.ru
Преподаватель факультета международных отношений
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан

В современной политике широко распространено убеждение в том, что процесс глобализации способствует быстрому развитию экономики, укреплению связей между государствами и народами в различных сферах общественной и политической жизни, а также научно-техническому прогрессу. Однако, научно-технический прогресс стал источником возникновения кибертерроризма. Понятие «кибертерроризм» объединяет два термина: «кибер», относящийся к виртуальному пространству для хранения и передачи данных, и «терроризм», имеющий международное значение. Интернет представляет собой идеальное поле для действий террористических организаций, которые используют современные технологии для своих целей, включая создание собственных веб-сайтов или аккаунтов в социальных сетях. Ряд факторов, таких как свободный доступ в сеть из любой точки мира, конфиденциальность передачи информации на большие расстояния, возможность создания и поддержания имиджа, пропаганда и легкодоступность в создании собственных онлайн-платформ, способствуют возникновению проблемы кибертерроризма в современном обществе.

В научной литературе выделяются два подхода к пониманию кибертерроризма. Первый подход основывается на использовании информационных технологий, включая социальные сети, для вербовки новых членов террористических организаций и популяризацию террористической деятельности. Несмотря на блокировку подобных сайтов, в Интернете все еще можно найти страницы таких террористических групп, как «Талибан», «Хамас», «Хезболла», «Черные тигры» и другие. Однако этот подход не охватывает всю сущность кибертерроризма, сосредотачиваясь лишь на его информационной составляющей. Второй подход к пониманию кибертерроризма основывается на определении кибертерроризма как формы терроризма, имеющей специфическое

место совершения — информационное пространство. В этом контексте объектом атак является информационная инфраструктура государств и международных организаций, а также виртуальные системы управления потенциально опасными или социально-значимыми объектами. Данный подход считается более точным, поскольку на современном этапе преступники используют информационные технологии не только для вербовки, коммуникации и передачи информации, но и как непосредственное средство совершения преступлений.

Преимуществом данного определения является то, что оно позволяет выявить все основные характеристики кибертерроризма. В первую очередь, кибертерроризм, как форма терроризма, направлен на достижение политических целей, таких как дестабилизация работы государственных органов власти, оказание на них давления и причинение ущерба мирному населению. Такие противоправные действия могут осуществляться как коллективами, так и отдельными лицами. И, наконец, местом для осуществления кибератак всегда будет выступать информационное пространство. Важно отметить, что основной проблемой, мешающей эффективному международному взаимодействию в борьбе с кибертерроризмом, является недостаток нормативного регулирования как на международном уровне, так и на уровне отдельных государств.

Кибертерроризм в настоящее время представляет собой полноценное оружие, поскольку использует информационные технологии, программные обеспечения и компьютерные системы, специально разработанные дестабилизации мирового сообщества и ведения террористической деятельности. Данный вид терроризма характеризуется низкими финансовыми затратами и способностью причинить огромный материальный ущерб противнику. Отсчет актов киберпреступности можно начать с 1970-х годов. Так, в 1973 г. кассир нью-йоркского Ситибанка, перевел на свой счет 2 млн. долларов, использовав служебный компьютер, а в 1989 г. американским студентом было заблокировано около 6000 ЭВМ Пентагона, но это было только и по некоторым меркам можно считать детской шалостью.[1] Так как с развитием интернета и всех технологий, сопутствующих ему, трагедии и последствия могут становиться все ужаснее, а идеи и методы все изощрение.

В настоящее время эксперты по информационной безопасности и противодействию киберпреступности выделяют три уровня кибертерроризма:

1. Неструктурированный уровень кибертерроризма включает использование хакерских методов против информационных систем с помощью программ, созданных третьими лицами, а не самими кибертеррористами. Обычно такие атаки являются простыми и могут привести к минимальным или незначительным потерям.
2. Расширенный уровень кибертерроризма предполагает структурированные действия, которые могут включать в себя более сложные атаки на несколько систем или сетей, а также возможность модификации или создания новых инструментов для взлома. Организация имеет определенную структуру, управление и другие характеристики, типичные для полноценных организаций. Участники таких группировок также обучают новичков-хакеров.
3. Комплексные – координированные: действия могут привести к массовым нарушениям систем безопасности страны, так как они способны провести сложные атаки и создать инструменты взлома. Такие группировки обладают четкой структурой и способны анализировать свои действия, разрабатывать планы атак и принимать другие стратегические решения.

Согласно отчету Лаборатории Касперского, чаще всего подвергаются киберугрозам США, Россия, Великобритания, Китай, Вьетнам, Индия и другие. Специалисты отмечают, что основными объектами интереса кибертеррористов являются военная и ядерная сферы, энергетика, финансы, а также транспортные перевозки [2].

Угроза кибертерроризма требует сотрудничества на межгосударственном уровне. В 2001 году Совет Европы принял «Конвенцию о преступности в области компьютерной информации», которая является ключевым документом в борьбе с киберпреступностью. Один из основных

способов международного сотрудничества в противодействии киберпреступности заключается в учреждении специализированных органов, таких как Интерпол, Европол и Евроюст. Евроюст координирует действия правоохранительных органов различных стран по вопросам расследования киберпреступности, оказывает помощь в проведении расследований по запросу соответствующего органа публичной власти стран-участниц ЕС и предоставляет информацию о проводимых расследованиях в отношении киберпреступников правоохранительным органам этих стран. Международное сотрудничество в данной сфере включает в себя также создание различных международных организаций, главной целью которых является пресечение действий организованных преступных сетей. Так, в 2013 г. в Гааге был открыт Европейский центр по борьбе с киберпреступностью, который собирает и обрабатывает материалы по киберпреступности, а также разрабатывает меры по их расследованию. В 2015 г. Интерпол инициировал открытие Международного центра по борьбе с киберпреступностью в Сингапуре. Перечисленные организации выявляют и проводят анализ киберугроз и IT-преступлений, а также обмениваются глобальным передовым опытом по борьбе с преступностью в киберпространстве.

Еще одним значимым документом является Резолюция ООН по борьбе с преступным использованием информационных технологий, принятая в 2001 году. Эта резолюция определила необходимые шаги для борьбы с киберпреступностью, такие как установление ответственности за компьютерные преступления, межгосударственное сотрудничество правоохранительных органов, обеспечение защиты компьютерных систем и сбор доказательств при расследовании киберпреступлений.

В ответ на вопрос о главных угрозах, стоящих перед человечеством в настоящее время, Генеральный секретарь ООН Антониу Гутерриш выделил терроризм, включая также компьютерный.

НАТО активно участвует в международной борьбе с киберпреступностью. В 2013 году была завершена разработка единой системы реагирования на кибератаки, аналогичные центры были созданы в Брюсселе и Монсе[3]. Постоянно проводится оценка эффективности действующей системы предупреждения кибератак, а также разрабатываются меры по ее улучшению. Ежегодно проводятся учения «Киберкоалиция» и «Защитный шар».

В начале 2015 года страны — участницы Шанхайской организации сотрудничества разработали и внесли на рассмотрение Генеральной ассамблеи ООН Кодекс поведения в области информационной безопасности, включающий правила поведения в киберпространстве на международном уровне. Также стоит отметить, что с 2015 года ШОС проводит учения по противодействию кибертерроризму раз в два года. В рамках этих учений создаются сценарии неизвестных кибератак на системы безопасности стран, где международная террористическая группировка пытается завербовать новых сторонников и распространять экстремистскую информацию. Благодаря таким учениям спецслужбы ШОС проверяют свою готовность и способность выявлять и предотвращать случаи кибертерроризма. В 2022 г., по результатам исследований, ШОС была выделена в качестве одной из организаций, которые внесли большой вклад в развитие системы международной информационной безопасности [4].

В конце 2018 года Генеральной ассамблеей ООН была принята резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», подписанная 119 странами.

Организационные меры по борьбе с кибертерроризмом принимаются и на национальных уровнях. Действующее законодательство по борьбе с кибертерроризмом в Казахстане включает в себя:

- Кодекс Республики Казахстан об административных правонарушениях от 5 июля 2014 года №235-V ЗРК;
- Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности РК;

- Уголовный кодекс Республики Казахстан «О противодействии терроризму» от 13 июля 1999 года № 416 со всеми дополнениями;
- Закон Республики Казахстан от 11 января 2007 года № 217-III «Об информатизации»;
- Закон Республики Казахстан от 21 мая 2013 года № 94-V «О защите персональных данных»;
- Концепцию «Киберщит Казахстана».

Концепция кибербезопасности, известная как "Киберщит Казахстана", была разработана в соответствии с Посланием Президента Республики Казахстан "Третья модернизация Казахстана: Глобальная конкурентоспособность" с учетом подходов Стратегии "Казахстан-2050" по вхождению Казахстана в число 30-ти самых развитых государств мира. Реализация данной Концепции способствует совершенствованию общества Казахстана и является вкладом страны в осуществление Глобальной программы кибербезопасности ООН[5].

Несмотря на уже предпринятые шаги, борьба с киберпреступностью на международном уровне сталкивается с рядом значительных проблем: каждая страна закладывает разное значение базовым определениям и понятиям; государства часто занимают разные позиции по вопросам защиты персональных данных; отсутствуют четкие границы между различными явлениями, требующими разных механизмов сотрудничества на международном уровне. Все это достаточно сильно затрудняет межгосударственное сотрудничество в условиях высокого взаимного недоверия.

В заключении можно отметить, что кибертерроризм представляет серьезную угрозу для мирового сообщества, поскольку он использует современные информационные технологии для достижения своих целей. Недостаток нормативного регулирования как на международном, так и на национальном уровнях затрудняет борьбу с этим видом преступности. Необходимо усилить усилия по разработке и внедрению эффективных механизмов защиты информационной инфраструктуры, а также укрепить международное сотрудничество для более эффективного противодействия кибертерроризму. Важно осознавать, что кибертерроризм требует комплексного подхода и совместных усилий со стороны всех заинтересованных сторон для обеспечения безопасности в киберпространстве.

Список использованных источников

1. Повышев В. Борьба с киберприступностью и кибертерроризмом. [Электронный ресурс]. URL:http://tmun.utmn.ru/wp-content/ uploads/SPChKiber.pdf (Дата обращения: 03.03.2024)
2. Интерактивная карта киберугроз: [Электронный ресурс]. URL: https://cybermap.kaspersky.com/ru/stats (Дата обращения: 08.03.2024).
3. Градов А. Деятельность Североатлантического союза в сфере кибербезопасности // Зарубежное военное обозрение. 2014. № 7. С. 13–16.
4. Якимова Е. М., Нарутто С. В. Международное сотрудничество в борьбе с киберпреступностью // Всероссийский криминологический журнал. 2016. Т. 10. № 2. С. 369–378.
5. Галицына А. Э., Кембель О. В., Потапова Д. Д. Региональное сотрудничество стран Центральной Азии в борьбе с кибертерроризмом // Постсоветские исследования. 2023. №6. С.626-638.

ӘОЖ 328

ЖАПОНИЯНЫҢ ОРТАЛЫҚ АЗИЯ АЙМАҒЫНДАҒЫ СЫРТҚЫ САЯСАТЫ

Шадаева Шолпан Абайқызы
shopik-8989@mail.ru