КИБЕРТЕРРОРИЗМ НА ПОСТСОВЕТСТКОМ ПРОСТРАНСТВЕ / CYBERTERRORISM IN THE POST-SOVIET REGION

Научная статья / Research article

Проблема борьбы с терроризмом в киберпространстве в Республике Казахстан

М. А. Зиновин

Российский университет дружбы народов им. П. Лумумбы, Москва, Россия
e-mail: azinoff@mail.ru

В. А. Данилов

Российский университет дружбы народов им. П. Лумумбы, Москва, Россия
e-mail: danilov_va@pfur.ru

Аннотация. С развитием интернет-технологий своё развитие и даже новую жизнь получили многие аспекты человеческой жизни: медицина, образование, новые виды работ и увлечений, но, в этот список также попала преступность и другие виды деятельности, которые направлены на дестабилизацию и крах гражданского общества. Кибертерроризм за последние десятилетия настолько усугубился, что стал одной из самых актуальных проблем в мире современных международных отношений, охватывая при этом многие регионы, включая постсоветское пространство. Казахстан, как и другие страны СНГ, не стала исключением. В данной статье авторы видят своей главной целью выявить основные проблемы при противодействии терроризму в киберпространстве на территории Казахстана. Хронологические рамки исследования затрагивают период с 2001 по 2022 гг., когда Казахстан впервые подвергся масштабной кибератаке. В статье анализируется, связанное с проблематикой кибертерроризма, законодательство Казахстана и правовые основы противодействия киберпреступлениям. Особое внимание в статье уделено анализу совершенных кибератак на государственные и иные интернет-ресурсы в стране. Авторы приходят к выводу о том, что в стране достаточно высокий уровень террористической активности в киберпространстве, что отчасти объясняется неэффективностью применения современных технологий защиты информации и недостаточным уровнем кибербезопасности в организациях и учреждениях. Кроме того, отсутствие строгих мер по контролю за использованием интернета и социальных сетей способствует усилению террористической пропаганды и вербовки новых сторонников. В связи с этим, необходимо проводить активную работу по улучшению кибербезопасности в стране, внедряя новые технологии и проводя обучение населения основам безопасного поведения в сети. Результаты данного исследования могут быть полезны для правительства, специалистов по кибербезопасности и всех, кто заинтересован в борьбе с терроризмом в киберпространстве на территории Казахстана.

Ключевые слова. Кибертерроризм, киберпреступления, Казахстан, противодействие кибертерроризму, СНГ.

Для цитирования: Зиновин М.А., Данилов В.А. Проблема борьбы с терроризмом в киберпространстве в Республике Казахстан // Постсоветские исследования. 2023;6(6):617-625.

The problem of countering terrorism in cyberspace in the Republic of Kazakhstan

Maxim A. Zinovin

RUDN University named after P. Lumumba, Moscow, Russia
e-mail: azinoff@mail.ru

Vitaly A. Danilov

RUDN University named after P. Lumumba, Moscow, Russia
e-mail: danilov_va@pfur.ru

Abstract. With the development of internet technologies, many aspects of human life have received a new lease on life: medicine, education, new types of work and hobbies. Unfortunately, crime and other activities aimed at destabilizing and destroying civil society have also made their way onto this list. Cyberterrorism has worsened over the past few decades and has become one of the most pressing issues in modern international relations, affecting many regions, including the post-Soviet space. The Republic of Kazakhstan, like other CIS countries, is not exempt from this list. The authors of this article aim to identify the main problems in combating terrorism in cyberspace on the territory of the Republic of Kazakhstan. The chronological framework of the study covers the period from 2001 to 2022, when Kazakhstan was first subjected to a large-scale cyberattack. The article analyzes the legislation of the Republic of Kazakhstan related to the problem of cyberterrorism and the legal basis for combating cybercrime. Special attention is paid to the analysis of cyberattacks on state and other internet resources in the country. The authors conclude that there is a sufficiently high level of terrorist activity in cyberspace in the country, partly due to the ineffective use of modern information protection technologies and insufficient levels of cybersecurity in organizations and institutions. In addition, the absence of strict measures to control the use of the internet and social networks contributes to the strengthening of terrorist propaganda and recruitment of new supporters. In this regard, it is necessary to actively work on improving cybersecurity in the country, introducing new technologies and conducting training for the population on the basics of safe behavior online. The results of this study can be useful for the government, cybersecurity specialists, and anyone interested in combating terrorism in cyberspace on the territory of the Republic of Kazakhstan.

Key words: Cyberterrorism, cybercrime, Republic of Kazakhstan, countering cyberterrorism, CIS.

For citation: Zinovin M.A., Danilov V.A. The problem of countering Terrorism in cyberspace in the Republic of Kazakhstan // Postsovetskie issledovaniya = Post-Soviet Studies. 2023;6(6):617-625. (In Russ.).

Кибертерроризм представляет серьезную угрозу для национальной безопасности многих стран по всему миру. Террористы могут использовать различные формы кибератак для дестабилизации экономики, криминальной деятельности, шпионажа и многого другого. Кроме того, развитие новых технологий и появление новых уязвимостей в компьютерных сетях создают дополнительные риски, которые следует учитывать при разработке мер по защите государственных структур и критической инфраструктуры. Еще больше волнений вызывает быстрое развитие технологий из-за чего кибертерроризм становится все более сложной и опасной проблемой.

Освещение проблематики, связанной с кибертерроризмом, является как никогда актуальным в научных работах в настоящее время. Научные исследования могут помочь в выявлении уязвимостей в системах безопасности, создании новых методов защиты от кибератак, а также в разработке стратегий борьбы с кибертерроризмом. Кроме того, научные работы могут стать основой для разработки законодательства, направленного на борьбу с будущими угрозами в сфере кибербезопасности.

Проблема борьбы с кибертерроризмом является серьезным международным вызовом и требует согласованного подхода, координации усилий и совместного решения ряда стран. Научные исследования могут сыграть важную роль в развитии стратегии и тактики противодействия этому явлению. Они помогут определить основные направления действий, выявить технические и организационные меры по повышению уровня безопасности информационных систем, защите государственных интересов и защите прав и свобод граждан [Власов 2021: 2].

Кибертерроризм: определение, виды, причины и основные отличия от терроризма

Терроризм, согласно закону Республики Казахстан "О противодействии терроризму" от 13 июля 1999 года № 416, Главы 1., Статьи 1 - это противоправное уголовно наказуемое деяние или угроза его совершения в отношении физических лиц или организаций в целях нарушения общественной безопасности, устрашения населения, оказания воздействия на принятие государственными органами Республики Казахстан, иностранными государствами и международными организациями решений либо с целью прекращения деятельности государственных либо общественных деятелей или из мести за такую деятельность[1]. Кибертерроризм, в свою очередь, использует современные интернет-технологии и уязвимости онлайн систем для достижения несколько иных целей, и имеет отличные от терроризма мотивы. [Бураева 2017: 1]. Он может включать в себя кибершпионаж, кибератаки на критическую инфраструктуру, распространение вредоносных программ, вымогательство взамен на прекращение кибертеррора, шантаж высокопоставленных лиц и т.д. [Вехов 1998: 29–37]. Данные методы чаще используются для финансового обогащения, реже мести[2,3], как это было указано выше. Не исключено, что средства, полученные за счет кибератак, затем пойдут на реализацию терактов в стране или на развитие террористической организации за счет вербовки новых участников или объединения с другими организациями [Мазуров 2010: 4].

Можно выделить несколько причин, по которым сеть Интернет привлекает террористические организации:

- доступность;
- отсутствие должного контроля со стороны государства;
- наличие неограниченного числа пользователей, на которых возможно оказать влияние;
- сложная идентификация личности;
- способность мгновенно распространять информацию по всему миру [Ленский 2017: 5].

Учитывая все, что было указано выше, основное отличие терроризма от кибертерроризма заключается в последствиях, которые следуют после соответствующих атак. Для примера были взяты два теракта:

1. Теракт в Алма-Ате 18 июля 2016 года. Пострадало 8 человек, 11 погибло[4].

2. В 2014 году произошла крупнейшая кибератака на банки Казахстана при помощи Zbot и параллельно с этим обычные жители Казахстана подверглись кибератаке через мобильные вирусы[5], в результате которых были украдены десятки миллионов долларов[6].

Как мы можем видеть, последствия двух видов атак кардинально отличаются друг от друга, но при этом обе эти атаки считаются террористическими актами, вне зависимости от кто был исполнителем и какие цели они преследовали.

Кибертерроризм в Республике Казахстан

История кибертерроризма в Казахстане началась с 2000-х гг., когда появились первые случаи кибератак на банки и другие объекты. Одним из первых таких случаев стало нападение на сайт компании "Kcell" в 2001 г.,

[1] Закон Республики Казахстан "О противодействии терроризму" от 13 июля 1999 года № 416 // Антитеррористический центр государств – участников Содружества Независимых Государств.URL: https://cisatc.org/1289/9115/135/9126/155/281/7914 (дата обращения: 04.04.2023).

[2] Казахстан подвергается масштабной кибератаке // Anadolu Ajansi СМИ. URL: https://goo.su/DVaJy (дата обращения: 04.04.2023).

[3] На Казнет продолжаются масштабные кибератаки // Kazakhstan Today СМИ. URL: https://www.kt.kz/rus/science/na_kaznet_prodolzhayutsya_masshtabnye_kiberataki_1377940471.html (дата обращения: 04.04.2023).

[4] Атака алматинского стрелка: что творилось на улицах во время теракта // Sputnik Казахстан СМИ. URL: https://ru.sputnik.kz/20180718/almatinskij-strelok-den-terakta-6479800.html (дата обращения: 04.04.2023).

[5] Казахстан оказался на 3-м месте среди самых атакуемых мобильными вирусами стран // Tengri News СМИ. URL: https://tengrinews.kz/internet/kazahstan-okazalsya-3-m-meste-sredi-samyih-atakuemyih-259795/ (дата обращения: 04.04.2023).

[6] На Казнет продолжаются масштабные кибератаки // Tengri News СМИ. URL: https://tengrinews.kz/internet/kiberataki-v-kazahstane-ugrojali-80-protsentam-kompaniy-256785/ (дата обращения: 04.04.2023).

когда неизвестные хакеры заблокировали доступ к сайту и потребовали выкуп [7]. В последующие годы наблюдалось увеличение числа кибератак на различные объекты в Казахстане, включая государственные и частные организации, мы выделили самые известные из них:

- В 2003 г. была зафиксирована серия DDoS-атак на казахстанские интернет-ресурсы, в том числе на сайты правительства и банков.
- В 2005 г. была произведена атака на сайт Центрального банка Казахстана, которая привела к временной недоступности ресурса.
- В 2008 г. произошла одна из самых масштабных кибератак на Казахстан - хакеры атаковали сайты правительства, банков и коммерческих организаций. Атаки были проведены при помощи ботнетов, созданных на компьютерах пользователей с использованием вредоносных программ. Схожие атаки можно было наблюдать на Украине, в Эстонии и Грузии.
- В 2014 г. каждый второй казахстанский пользователь был атакован хакерами[8].
- В мае 2017 г. была проведена кибератака на сервера оператора Кашагана (морское месторождение нефти), которая прервала добычу нефти на этом месторождении на несколько месяцев. Добыча нефти на гигантском морском месторождении Кашаган в Атырауской области была возобновлена осенью 2017 г.[9] В этом же году банковский сектор страны вновь был атакован, некоторые эксперты называют атаки беспрецедентными и заявляют о том, что это только начало.[10]
- В 2019 г. была проведена кибератака на Национальный банк Казахстана, в результате которой были украдены конфиденциальные данные о клиентах банка. Также в этом же году была зафиксирована кибератака на систему энергоснабжения Астаны и на сайт аэропорта Астаны из-за чего в адрес руководства аэропорта посылался шквал негативных отзывов, тем самым подорвав доверие к сервису.[11]
- В 2020 г. произошла серия кибератак на крупные компании Казахстана, в том числе на Национальную компанию «Қазақстан темір жолы» и компанию «Казахтелеком». Было заявлено, что за атаками стояли зарубежные хакерские группировки.
- Согласно отчету KPMG «Drilling Down» случаи атак программ-вымогателей на сети ОТ увеличились в пять раз с 2018 по 2020 год. Из них на производственные предприятия приходится более трети подтвержденных атак программ-вымогателей, за ними следуют коммунальные службы, на долю которых приходится 10%. Количество атак программ-вымогателей резко возросло, в 2021 г. ущерб от них достиг 20 млрд долл. по сравнению с 0,3 млрд долл. в 2015 г. В 2020 г. число атак программ-вымогателей на энергетические и коммунальные предприятия увеличилось на 32 %[12]
- В 2022 г., в связи с началом электорального периода в Казахстане, проводилась массированная атака на

[7] Произошедший сбой сотовой связи в сети K`CELL // КАРАВАН Медиа-портал. URL: https://www.caravan.kz/news/proizoshedshijj-sbojj-sotovojj-svyazi-v-seti-kcell-ne-imel-politicheskojj-podopleki-glava-kompanii-gsm-kazakhstan-170558/ (дата обращения: 05.04.2023).

[8] Кибератаки в Казахстане угрожали 80 процентам компаний // Tengri News СМИ. URL:https://tengrinews.kz/internet/kiberataki-v-kazahstane-ugrojali-80-protsentam-kompaniy-256785/ (дата обращения: 05.04.2023).

[9] Хакеры атаковали серверы оператора Кашагана // Капитал Казахстан СМИ. URL: https://kapital.kz/economic/59747/khakery-atakovali-servery-operatora-kashagana.html

[10] Кто устроил кибератаки на банки и пытался обчистить казахстанцев // Informburo.kz СМИ. URL: https://informburo.kz/stati/kto-ustroil-kiberataki-na-banki-i-pytalsya-obchistit-kazahstancev.html

[11] Хакеры подорвали доверие к сайту аэропорта Астаны - программист // Sputnik Казахстан СМИ. URL:https://ru.sputnik.kz/20190305/khaker-ataki-satiyev-9511763.html (дата обращения: 05.04.2023).

[12]Годовой отчет 2022 АО НК «КазМунайГаз» // Отчет газовой компании. URL:https://www.kmg.kz/upload/iblock/af5/rn8yccb2p6yx9tqufp5b31ea5h893kj5/KMG_AR2022_RUS%20(1).pdf (дата обращения: 05.04.2023)

«Казнет» и государственные компании и интернет-ресурсы. Согласно данным полученным от АО "Государственная техническая служба" (АО "ГТС"), с 5 сентября по 5 октября 2022г. – было отражено около 20 млн кибератак.[13]

Проанализировав представленные выше кибератаки, выделив в них угрозы и уязвимости для киберпространства Казахстана, можно сделать вывод, что основными уязвимыми местами являются критически важные государственные системы, такие как системы энергоснабжения, транспорта, телекоммуникаций, объекты государственного управления и банки. В добавок к этому можно провести некую параллель между атаками и развитием интернета в стране. Казнет в самом начале имел невероятный потенциал развития и находился в лидерах мировой паутины [Темирболат Бакытжан 2010: 5-7]. Согласно данным, полученным с сайта посвящённому развитию интернета на территории Республики Казахстан [14] (см. рис. 1-3). Основные этапы развития Казнета совпали с периодами кибертеррора в стране, что говорит о том, что до появления «Киберщита Казахстана» в 2017 г., правительство не имело возможности противостоять теневой интернет мафии, которая с 2000-х гг. нанесла ущерб не только Казахстану и каждой стране в мире, которая была подключена к мировой сети интернет.

Однако, несмотря на комплекс мер, проводимых государством, по противодействию кибертерроризму, недавний отчет специалистов из «Лаборатории Касперского» говорит о том, что количество фишинговых атак в Казахстане увеличилось на 12% в первом квартале 2023 г. по сравнению с аналогичным периодом прошлого года. При этом корпоративный сектор стал наиболее уязвимым и был подвержен фишинговым атакам с ростом в 120%. Специалисты компании рассчитали, что Казахстан занимает седьмое место в мире по количеству кибератак.[15]

Противодействие кибертерроризму в Республике Казахстан

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»
- Концепция «Киберщит Казахстана»

В 2007 г. в законодательстве Казахстана появились такие понятия как персональные данные, их сбор и распространение (Закон «Об информатизации»). Затем в 2013 г. был разработан закон "О персональных данных и их защите" целью которого является обеспечение защиты прав и свобод человека и гражданина при сборе и обработке персональных данных. Оба этих закона регулирует отношения, связанные со сбором, обработкой и защитой персональных данных граждан Казахстана.

Незадолго до создания концепции киберщита, в 2016 г. прошел форум хакеров «DEFCON», на котором впервые появилась казахская группа, инициированная Центром анализа и расследоваия кибератак (ЦАРКА).

[13] Киберщит Казахстана отразил около 20 млн атак за месяц// Zakon.kz СМИ. URL: https://www.zakon.kz/6026731-kibershchit-kazakhstana-otrazil-okolo-20-mln-atak-za-mesiats.html (дата обращения: 05.04.2023).

[14] История мировой паутины // Сайт-архив. URL: http://bluescreenkz.tilda.ws/page24552755.html (дата обращения: 08.04.2023).

[15] Казахстан занял седьмое место в мире по количеству кибератак // Forbes Kazakhstan Журнал. URL: https://forbes.kz/actual/technologies/kaspersky_kazahstan_zanyal_sedmoe_mesto_v_mire_po_kolichestvu_kiberatak (дата обращения: 08.04.2023).

На этой встрече прозвучали заявления о том, что Казахстан абсолютно не готов к информационной войне и кибератакам. Об этом заявили участники первой встречи «этичных хакеров» в Астане, наглядно продемонстрировав уязвимости порталов гос.органов и частных компаний. О казахстанцах, как и обо всех пользователях интернета, постоянно собираются данные и при любом удобном случае, их могут использовать в ущерб национальным интересам страны, поэтому государству и рядовым пользователям нужно научиться защищать информацию.[16]

После таких громких заявлений, 7 марта 2017 года правительство Казахстана представила свою концепцию «Киберщит Казахстана» [17] . Эта концепция определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий.[18]

15 марта этого же года эксперты высказали свои рекомендации по улучшению правительственной концепции. В ходе обсуждения выяснилось, что существовавшая на тот период времени интернет инфраструктура в стране не позволяет реализовать эту концепцию. Согласно мнению Армана Абдрасилова, директора Центра анализа и расследования кибератак, проект Концепции создания национальной системы кибербезопасности является недоделанным документом, который не отражает важных вопросов по созданию «Киберщита». Он считает, что проект не содержит описания составных частей системы и их функций. Эксперт также не соглашается с тем, что система мер по обеспечению кибербезопасности уже сформирована и законодательно закреплена, ссылаясь на отсутствие единой системы мер и документов, объединяющих меры и закрывающих отдельные вопросы. «К тому же в Казахстане острой проблемой является слабое развитие отечественной индустрии информационной безопасности, в частности в разработке средств криптографии. Одна из причин такой ситуации в том, что иностранные компании-гиганты через своих представителей в республике не дают возможности встать на ноги отечественным специалистам и компаниям. С учетом того, что разработки в области защиты информации напрямую связаны с обеспечением госсекретов, использование готовых иностранных продуктов крайне опасно, необходимо развивать собственные лаборатории», - подчеркивает Ержан Сейткулов, директор НИИ информационной безопасности и криптологии Евразийского национального университета им. Л.Н. Гумилева, член Общественного совета министерства оборонной и аэрокосмической промышленности Казахстана.[19]

Опираясь на полученную информацию, мы выделили основные направления развития методов по борьбе с кибератаками в Казахстане:

1. Обучение населения и сотрудников компаний основам кибербезопасности. Государственные структуры и частные компании должны организовывать тренинги и обучения сотрудников правилам безопасного поведения в сети.

2. Первоначально необходимо усиление защиты критической инфраструктуры, такой как электростанции, водоочистные и другие объекты, которые ранее неоднократно были атакованы и будут атакованы в будущем.

3. Развитие существующей инфраструктуры для обнаружения и

[16] Первая DEFCON встреча вскрыла проблемы в национальной кибероборонe Казахстана // Digital.Report СМИ. URL: https://digital.report/pervaya-defcon-vstrecha-vskryila-problemyi-v-natsionalnoy-kiberoborone-kazahstana/ (дата обращения: 08.04.2023).

[17] Опубликована концепция «Киберщит Казахстана» // Digital.Report СМИ. URL: https://digital.report/opublikovana-kontseptsiya-kibershhit-kazahstana/ (дата обращения: 08.04.2023).

[18] Киберщит // Комитет национальной безопасности Республики Казахстан государственный сайт. URL: https://www.gov.kz/memleket/entities/knb/activities/250?lang=kk (дата обращения: 08.04.2023).

[19] «Киберщит Казахстана»: идеология & конкретика? // Информационная система ПАРАГРАФ архив. URL: https://online.zakon.kz/Document/?doc_id=36321387&pos=15;-48#pos=15;-48 (дата обращения: 08.04.2023).

реагирования на кибератаки. Это запуск дополнительных систем мониторинга, детектирования и аналитики, а также разработка плана действий для быстрого реагирования на кибератаку.

Заключение

Спустя 6 лет с момента появления Концепции «Киберщит Казахстана» государственные структуры все еще подвергаются огромному количеству кибератак, но несмотря на это, у Концепции есть бесконечное пространство для развития в будущем. Кроме того, в Казахстане есть компании, которые имею успешный опыт защиты своих данных. Так, например, для предотвращения киберрисков и утечки чувствительных данных «КазМунайГаз» проводит работу по поддержанию соответствия системы менеджмента информационной безопасности (СМИБ) действующим международным стандартам и аудит информационной безопасности. [20] Точно такую же работу должны проводить и другие крупные компании, дабы расширить консультационный ресурс для модификации гос. проектов по киберзащите. Кроме того, необходимо сотрудничать со всеми заинтересованными странами. Это может быть обмен информацией или координация действий при возникновении глобальных киберугроз.

ИЛЛЮСТРАЦИИ

Рисунок 1.

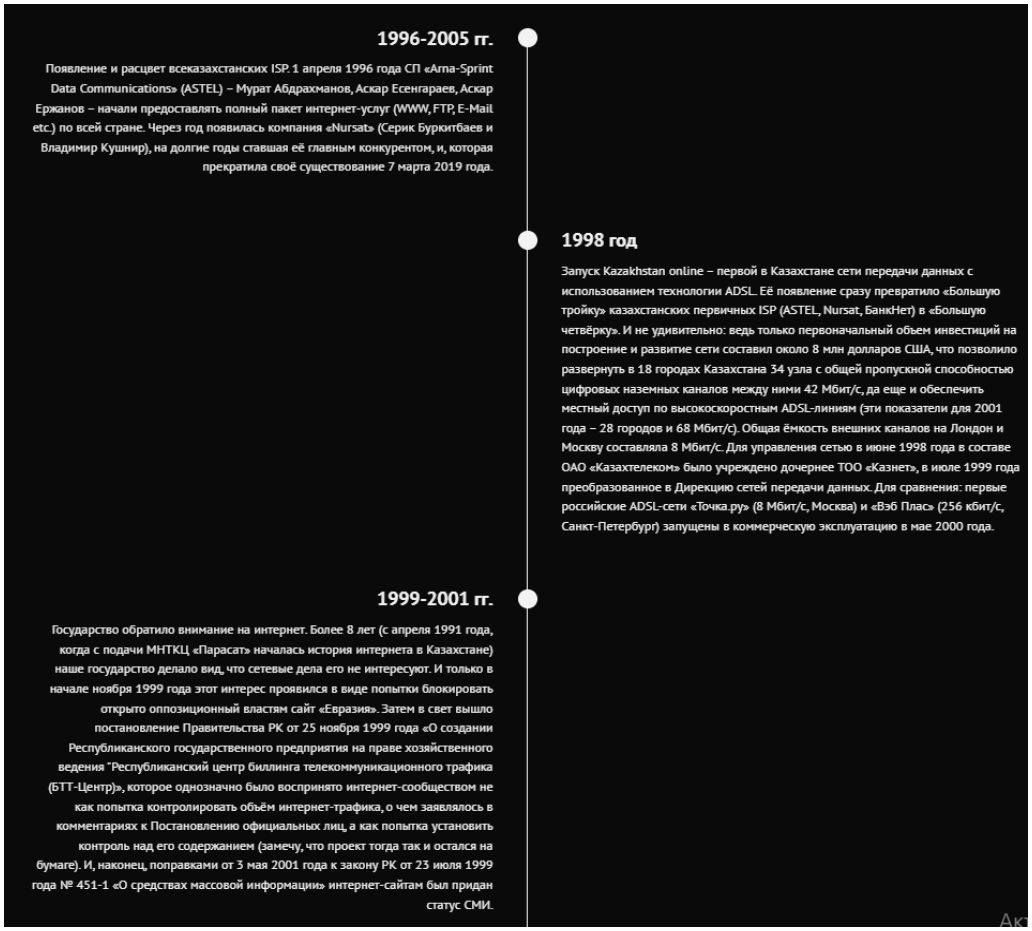

Рис. 1. История развития интернета в Республике Казахстан (1996-2001 гг.)[21]

[20] Годовой отчет 2022 АО НК «КазМунайГаз» // Отчет газовой компании. URL:https://www.kmg.kz/upload/iblock/af5/rn8yccb2p6yx9tqufp5b31ea5h893kj5/KMG_AR2022_RUS%20(1).pdf (дата обращения: 05.04.2023).

[21] Важные этапы истории Казнета // Сайт-архив. URL: http://bluescreenkz.tilda.ws/page24552755.html (дата обращения: 08.04.2023).

Рисунок 2.

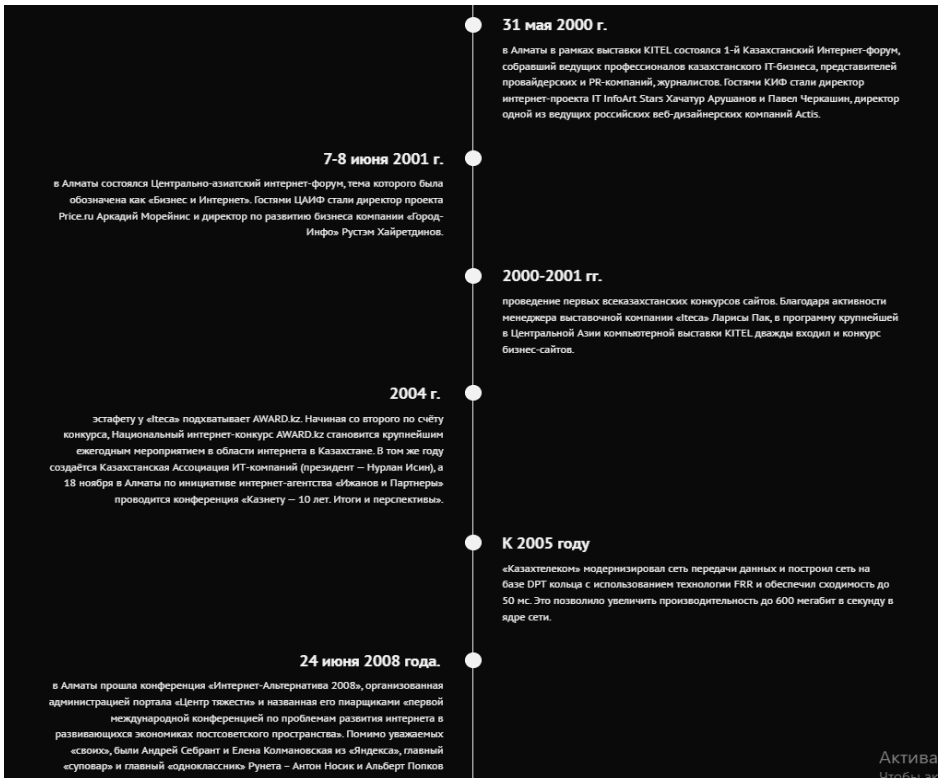

Рис. 2. История развития интернета в Республике Казахстан (2001-2008 гг.)[22]

Рисунок 3.

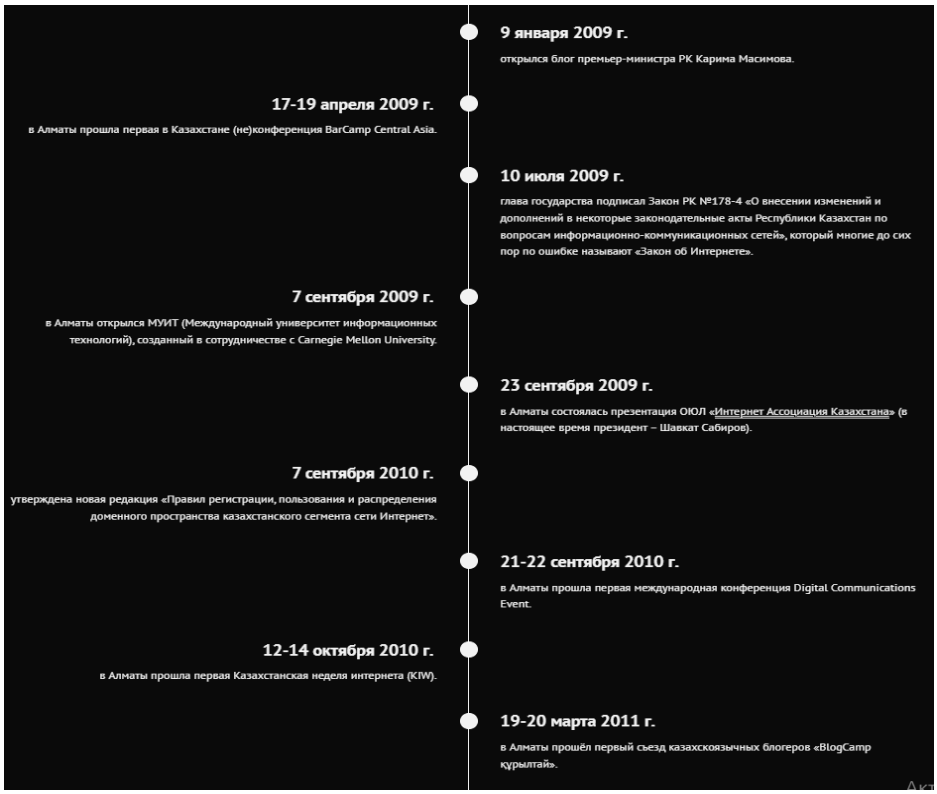

Рис. 3. История развития интернета в Республике Казахстан (2008-2011 гг.)[23]

[22] Важные этапы истории Казнета // Сайт-архив. URL: http://bluescreenkz.tilda.ws/page24552755.html (дата обращения: 08.04.2023).

[23] Важные этапы истории Казнета // Сайт-архив. URL: http://bluescreenkz.tilda.ws/page24552755.html (дата обращения: 08.04.2023).

СПИСОК ЛИТЕРАТУРЫ

Бураева Л. А. Кибертерроризм как новая и наиболее опасная форма терроризма // Пробелы в российском законодательстве. 2017. №3. С. 35-37.

Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. –М.: Право и закон, 1998. – С. 182.

Власов И. А. Проблемы борьбы с кибертерроризмом в современной России / И. А. Власов // Судебная система России на современном этапе общественного развития: Сборник научных трудов Всероссийской студенческой научной конференции, Ростов-на-Дону, 10 декабря 2021 г. – Ростов-на-Дону, 2021. – С. 399-402.

Ленский И. А. Кибертерроризм как одна из форм современного терроризма / И. А. Ленский // Актуальные вопросы тактики охраны общественного порядка и общественной безопасности: Сборник научных статей Материалы межвузовской научно-практической конференции, Иркутск, 27 января 2017 года. – Иркутск: Восточно-Сибирский институт МВД Российской Федерации, 2017. – С. 100-108.

Темирболат Бакытжан Политический Интернет в Казахстане: тенденции, проблемы и перспективы // Центральная Азия и Кавказ. 2011. №1. С. 179-192.

Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУР. 2010. №1-1 (21). С. 41-45.

REFERENCES

Buraeva L. A. Kiberterrorizm kak novaya i naiboleye opasnaya forma terrorizma // Probely v rossiyskom zakonodatel'stve. 2017. №3. P. 35-37.

Vekhov V.B. Komp'yuternyye prestupleniya: sposoby soversheniya, metodiki rassledovaniya. – M.: Pravo i zakon, 1998. – P. 182.

Vlasov I. A. Problemy bor'by s kiberterrorizmom v sovremennoy Rossii / I. A. Vlasov // Sudebnaya sistema Rossii na sovremennom etape obshchestvennogo razvitiya: Sbornik nauchnykh trudov Vserossiyskoy studencheskoy nauchnoy konferentsii, Rostov-na-Donu, December 10, 2021. – Rostov-na-Donu, 2021. – P. 399-402.

Lensky I. A. Kiberterrorizm kak odna iz form sovremennogo terrorizma / I. A. Lenskiy // Aktual'nyye voprosy taktiki okhrany obshchestvennogo poryadka i obshchestvennoy bezopasnosti : Sbornik nauchnykh statey Materialy mezhvuzovskoy nauchno- prakticheskoy konferentsii, Irkutsk, January 27, 2017. – Irkutsk: Vostochno- Sibirskiy institut MVD Rossiyskoy Federatsii, 2017. – P. 100-108.

Temirbolat Bakytzhan Politicheskiy Internet v Kazakhstane: tendentsii, problemy i perspektivy // Tsentral'naya Aziya i Kavkaz. 2011. №1. P. 179-192.

Mazurov V.A. Kiberterrorizm: ponyatiye, problemy protivodeystviya // Doklady TUSUR. 2010. №1-1 (21). P. 41-45.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Зиновин Максим Андреевич, студент 1 курса магистратуры, направление «международные отношения», РУДН им. П. Лумумбы, Москва, Россия. (E-mail: azinoff@mail.ru)

Данилов Виталий Алексеевич, к.и.н, директор центра прикладного анализа международных трансформаций, доцент кафедры теории и истории международных отношений РУДН им. П. Лумумбы, Москва, Россия. (E-mail: danilov_va@pfur.ru)

Maxim A. Zinovin, 1st year student of the master's program "international relations", RUDN University named after P. Lumumba, Moscow, Russia. (E-mail: azinoff@mail.ru).

Vitaly A. Danilov, Ph.D. in history, Director of the Center for Applied Analysis of International Transformations, Associate Professor of the Department of Theory and History of International Relations RUDN University named after P. Lumumba, Moscow, Russia. (E-mail: danilov_va@pfur.ru).