DOI 10.37882/2223-2974.2024.09.26

ОТЕЧЕСТВЕННЫЙ СУВЕРЕННЫЙ РУНЕТ И ЗАРУБЕЖНЫЕ МОДЕЛИ ИНТЕРНЕТ-БЕЗОПАСНОСТИ: СРАВНИТЕЛЬНО-ПРАВОВОЕ ИССЛЕДОВАНИЕ

THE DOMESTIC SOVEREIGN RUNET AND FOREIGN INTERNET SECURITY MODELS: A COMPARATIVE LEGAL STUDY

N. Mikhalenko

Summary. The article reveals the problem of information security in the Russian Federation. The author considers the concept of the Runet as a segment of the Internet regulated by Russian legislation. The statistical data related to the blocking of websites in the Russian Federation are presented. Also, the analysis of the EU's overall strategy on Internet security issues was carried out in a number of individual European countries (Denmark, Spain, Germany, France), as well as Asia (China). The trends of the state policy aimed at improving the security of the national Internet are revealed.

Keywords: Runet, legislation, security, strategy, cybercrime, Internet traffic.

Михаленко Никита Алексеевич
Аспирант, Федеральное государственное автономное образовательное учреждение высшего образования «Самарский государственный экономический университет»
bote2018@gmail.com

Аннотация. В статье раскрывается проблема информационной безопасности в Российской Федерации. Автором рассмотрено понятие Рунета как сегмента Интернета, регулируемого российским законодательством. Приведены статистические данные, связанные с блокировкой сайтов в РФ. Также, осуществлен анализ общей стратегии ЕС по вопросам Интернет-безопасности ряда отдельных стран Европы (Дания, Испания, Германия, Франция), а также Азии (Китай). Выявлены тенденции государственной политики, направленной на повышение безопасности национального Интернета.

Ключевые слова: Рунет, законодательство, безопасность, стратегия, киберпреступность, интернет-трафик.

Интернет стал неотъемлемой частью жизни каждого жителя планеты Земля, его роль в современном обществе пока еще не оценена окончательно. Вместе с его стремительным развитием актуализировались вопросы, связанные с информационной безопасностью государств. Как любое явление Интернет имеет положительные и отрицательные свойства, к первым можно отнести универсальность, глобальность и оперативность, а ко вторым — «использование сети как средства ведения информационной войны, возможность технического воздействия или контроля за пределами той или иной страны» [3, с. 85].

Под Рунетом понимается российский сегмент Интернета, представляющий собой «совокупность интернет-ресурсов, приложений, сервисов, сайтов, которые базируются на российских серверах и (или) расположены на доменах типа «рф.ru» [7, с. 20].

На этот сегмент Интернета и может воздействовать российский законодатель. Основной принцип такого воздействия заключается в необходимости регулирования российского «медиапространства государством, обществом и бизнесом» [2, с. 87].

Цифровизация один из приоритетов в развитии современного российского государства, отставание в этой сфере по сравнению с мировыми тенденциями может иметь отрицательные последствия. С цифровизацией тесно связано понятие кибербезопасность как одно из ключевых в данном направлении. «Кибербезопасность — способность защищать и оборонять киберпространство от кибератак» [8]. В свою очередь, установление кибероборонь необходимо для того, чтобы предотвратить киберугрозы.

Понимая важность этих процессов, правительство уделяет ему особое внимание и в данном случае многое зависит от законодательного регулирования.

Внесение в 2019 году поправок в федеральные законы «О связи», «Об информации, информационных технологиях и о защите информации» получили название и широко известны общественности как «закон о суверенном интернете» [1, с. 140].

Принятие таких правовых актов связано с необходимостью защитить российский сегмент и противостоять влиянию зарубежных стран и , прежде всего США, на киберпространство и цифровую экономику нашей страны. Для противостояния агрессивности Стратегии национальной кибербезопасности США (2018) в РФ создается национальная система маршрутизации интернет-трафика. В случае выявление угрозы и критического сбоя во внешней сети может быть введено централизованное управление Рунетом.

Согласно данным портала rknweb.ru на 24.07.2024 в РФ заблокировано более полмиллиона доменов, из них по решению ФНС — 190 тыс., на основании постановления суда — 118 тыс., на третьем месте — решения Роскомнадзора — 108 тыс. По сравнению с 2022 годом снизилось число блокировок со стороны Мосгорсуда до 30 тыс., и Генпрокуратуры — 19, 6 тыс. [6].

В настоящее время наблюдаются две тенденции со стороны государственных структур в правовом регулировании национального Интерната: «усиление государственного контроля над Интернетом или внедрение механизма саморегулирования отрасли» [5, с. 182].

Китай и Северная Корея, обладая особым политическим строем и экономическим устройством, смогли установить в своих странах систему закрытого Интернета. В Китае связь с внешним цифровым миром осуществляется при помощи трех «шлюзов», жестко контролируемых государством. Их оборудование размещено в Пекине, Шанхае и Гуанчжоу. Благодаря этому Пекин обезвредил страну от возможности вести кибервойну и киберразведку со стороны США. Принятый в 2017 г. в Китае закон о кибербезопасности, обязывал: все госучреждения использовать «безопасные» технологии; избавиться от иностранного «железа» и «софта»; осуществлять систему фильтрации трафика. Последнее дало возможность государству установить тотальный контроль над пользователями Интернета. Создав собственную национальную систему Интернета, страна занимает 33 место в глобальном рейтинге безопасности и 15 — в Национальном [10]. Китай обратился с предложением к странам БРИКС и ШОС создать собственную систему корневых серверов.

В современном мире только в Китае, занимающем первое место в рейтинге несвободного интернета, создана система, получившая название «Золотого щита» «исключительно с целью обеспечения информационной безопасности» [3, с. 84]. По мнению А.В. Куликовского китайский «Золотой щит» это не полноценная автономная сеть, а своего рода «железный занавес».

В России защитить Рунет с помощью виртуального щита вряд ли получится. Мнение экспертов по возможности отключения России от глобальной сети разделились: одни считают, что это маловероятно, другие не отрицают такую возможность» [4].

В России заблокированы зарубежные сервисы, такие как фейсбук, инстаграмм, буквально на днях отключен ютуб. Цель защиты государственных интересов в сфере кибербезопасности должна находиться в балансе с интересами прав граждан. В настоящее время в рейтинге несвободного интернета РФ занимает 5 место.

Проблемой безопасности Интернета обеспокоены и страны ЕС. Общая стратегия кибербезопасности ЕС была принята в декабре 2020 г. в Брюсселе и направлена на повышение устойчивости к киберугрозам. Она является флагманским документом, задающим определенный тренд для стратегий национальных государств. Интернет-пространство остается открытым, но государства дают своим гражданам надлежащие гарантии при его использовании и защиту от похищения персональных данных.

Приоритетными направлениями в рамках совместной деятельности ЕС стали:

— обеспечение интернет-устойчивости объектов социальной и оборонной сферы, путей сообщения, систем, связанных с обеспечением энергией и деятельностью органов госуправления;
— создание совместных киберподразделений в странах ЕС и координация их деятельности;
— «сотрудничество и партнерство в целях развития глобального и открытого киберпространства, основанного на международных нормах и стандартах» [8].

Страны ЕС не делятся информациях об инцидентах в сфере национального киберпространства, отсюда возникает необходимость создания киберподразделений как единой платформы для государств ЕС в плане обмена информацией с целью обеспечения независимости, в том числе технологической от других государств.

Сравним стратегии кибербезопасности ведущих стран Европы: Испании, Франции и Германии. В Глобальном индексе кибербезопасности согласно Аналитическому Отчету Экспертно-Аналитического центра InfoWatch за 2022 год Испания занимает 4 место, Франция — 9 место, Германия — 13 место» [8]. В количестве целей определения стратегии страны выглядят таким образом: Испания определила для себя 15 целей, Франция — 13, Германия — 9.

Стратегия кибербезопасности была принята Испанией в 2013 году, в 2019 была модернизирована. В этой стратегии стана определила для себя приоритетность кибербезопасности, виды угроз и их классификацию и выделила 7 направлений деятельности. Но стандартов кибербезопасности Испания не определила, не хватает ей и четкости в структурировании госуправления по данному вопросу, а также стимулировании бизнеса вкладывать средства в развитие кибербезопасности.

Во Франции Стратегия была принята в 2015 г. и включает в себя:

— контроль безопасности информационных технологий, усиление безопасности государственных информационных систем;

— защиту цифровой жизни граждан;
— помощь жертвам злоумышленников, осуществляющих свои действия в киберпространстве;
— особое внимание уделяется безопасности детей и молодежи в Интернете, для этого вопросы кибербезопасности включены в учебные программы.

Цифровизация безопасности рассматривается французским правительством как фактор конкурентноспособности. Государство играет активную роль в ЕС в создании дорожной карты для европейской стратегической автономии и готово оказывать добровольную помощь гражданам в создании систем кибербезопасности.

В законодательстве Франции есть понятие защиты объектов критической информационной инфраструктуры, это означает, что все поставщики жизненно важных услуг обязаны уведомлять ANSSI об инцидентах.

Франция стремится к лидерству в европейской кибероборонe. В 2019 году принята частично засекреченная доктрина «Наступательные военные действия в киберпространстве» [8].

Стратегия кибербезопасности Германии принята недавно в 2021 г. и ориентирована на совместную деятельность правительства, ученых, частного бизнеса и общества в данном направлении.

Для создания системы кибербезопасности намечены следующие цеди:
— повышение осведомленности и киберграмотности жителей страны, защита прав потребителей в цифровом мире;
— выстраивание архитектуры кибербезопасности для госуправления, в плане сотрудничества и повышении квалификации сотрудников госорганов;
— тесное сотрудничество правительство с представителями бизнеса;
— стремление к ключевой роли Германии в международной политике кибербезопасности.

Национальная стратегия кибербезопасности и информационной безопасности на 2022–2024 годы, принята правительством Дании в декабре 2021 года [9]. Она не имеет существенных отличий от стратегий других стран ЕС. Спрос на навыки кибербезопасности в северной стране достаточно высок и государство целенаправленно работает над повышением уровня знаний и навыков цифрового поведения и безопасности среди граждан с целью развития у них здоровых и безопасных цифровых привычек. Несмотря на предпринимаемые правительством меры и желанием граждан оставаться в безопасности в цифровом формате, Дания в ноябре 2023 г. подверглась мощнейшей хакерской атаке.

Современные тенденции развития глобальной сети свидетельствуют, что дальнейшая автономность Рунета будет способствовать снижению конкуренции для российских инфоисточников и сайтов, в связи с этим «некоторые зарубежные ресурсы могут стать недоступными для пользователей из России и, возможно, в перспективе — из ЕАЭС в целом» [3, с. 88].

На основе анализа отечественного и зарубежных моделей безопасности национального Интернета на взгляд автора представляется необходимым:
— объединить усилия государства, общества и бизнеса в части создания безопасного Рунета;
— ввести правила безопасного пребывания в Интернете и обучать им всех граждан, а особенно детей и подростков;
— разработать проект кодифицированного акта о российской сети Интернета.

ЛИТЕРАТУРА

1. Жуков А.З., Шугунов Т.Л. Внедрение закона о «суверенном рунете»: правовой и технический аспекты // Социально-политические науки. 2020. Т.Х. №2. С.139–142.
2. Корнев М.С., Тихонова Е.М. Механизмы регуляции и обеспечения информационной безопасности в современном Рунете // В сборнике: Взаимодействие вузов, научных организаций и учреждений культуры в сфере защиты информации и технологий безопасности. Сборник статей по материалам международной конференции, посвящённой памяти доктора технических наук, профессора А.А. Тарасова и доктора технических наук, старшего научного сотрудника О.В. Казарина. Москва, 2022. С. 83–92.
3. Куликовский А.В. Возможный запуск автономного Рунета и его роль в обеспечении информационной безопасности ЕАЭС// Вестник Таджикского государственного университета права, бизнеса и политики. Серия гуманитарных наук. 2021. № 2 (87). С. 83–90.
4. Медведев Д.: РФ может сделать Рунет автономным, но не хочет до этого доводить // URL: https://tass.ru/obschestvo/10587069 (Дата обращения: 05.08.2024).
5. Петрищева Е.Н., Лемайкина С.В. Правовые аспекты государственного регулирования Рунета // Юристъ-Правоведъ. 2017. № 3 (82). С. 177–183.
6. Статистика блокировок. Распределение по ведомствам // URL: https://rknweb.ru/statistics/ (дата обращения: 09.08.2024).
7. Слюсаренко Т.В., Савощикова Е.В. Выделение из мировой сети Рунета как нового поля правового регулирования российского законодательства // Вестник Московского университета им. С. Ю. Витте. Серия 2: Юридические науки. 2020. № 3 (25). С. 19–24.
8. Стратегии кибербезопасности государств Европейского Союза // URL: https://www.infowatch.ru/analytics/analitika/strategii-kiberbezopasnosti-gosudarstv-evropeyskogo-soyuza (дата обращения: 09.08.2024).
9. Denmark — National Strategy for Cyber and Information Security 2022–2024 Digital Skills and Jobs Platform. // URL: https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/denmark-national-strategy-cyber-and-information (дата обращения: 09.08.2024).
10. The 10 best (and worst) countries for cybersecurity // BBC Sienes focus // URL: https://www.sciencefocus.com/news/the-10-best-and-worst-countries-for-cybersecurity (дата обращения: 09.08.2024).

Журнал «Современная наука: актуальные проблемы теории и практики»