Коринь Виктория Владимировна
Студент 2 курса Института государства и права
Тюменского государственного университета
korinvv@gmail.com

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В КИТАЕ И В РОССИИ

Аннотация. В данной работе рассматривается законодательная политика Китая и России, связанная с обеспечением информационной безопасности и противодействию киберугрозам. Российская Федерация и Китайская Народная Республика одни из ведущих держав в цифровой области, вследствие чего возникает интерес узнать, какие нормативные акты изданы властями для обеспечения безопасности в сети. Также перечисляются органы власти, ответственные за кибербезопасность. Проводится сравнение правового обеспечения кибербезопасности этих стран на основе изданных нормативных документов и проводимой политики, а также обозначаются плюсы и минусы в системе каждого из двух государств. Приводятся варианты улучшения политики в информационной сфере, которые Россия и Китай могут перенять у друг друга, поскольку обе страны заинтересованы в усилении кибербезопасности.
Ключевые слова: Россия, Китай, кибербезопасность, обеспечение, закон.

Korin Victoria Vladimirovna
2nd year student of the Institute of State and Law
University of Tyumen

LEGAL SUPPORT FOR CYBERSECURITY IN CHINA AND RUSSIA

Abstract. This paper examines the legislative policy of China and Russia related to ensuring information security and countering cyber threats. The Russian Federation and the People's Republic of China are among the leading powers in the digital field, which leads to interest in finding out which regulations have been issued by the authorities to ensure security on the network. The authorities responsible for cybersecurity are also listed. A comparison is made of the legal provision of cybersecurity in these countries on the basis of published regulatory documents and policies, as well as the pros and cons in the system of each of the two states. The paper presents options for improving information policy that Russia and China can adopt from each other, since both countries are interested in strengthening cybersecurity.
Key words: Russia, China, cybersecurity, security, law.

Современный мир трудно представить без цифрового формата жизни. Появляются новые возможности, неведанные людям до это-

го. Возникло глобальное информационное пространство с различными структурами, которые содержат в себе множество данных: лично каждого человека, всего государства.

Вместе с новыми возможностями возникают проблемы, которые посредством использования информационных структур несут опасность миру. Появляющиеся проблемы и угроза информационных войн требуют определенные меры защиты. Страны разрабатывают законы и другие нормативные документы, которые позволят обеспечить кибербезопасность своим государственным ресурсам и своему населению.

В данной работе будут проанализировано и сопоставлено правовое обеспечение кибербезопасности двух стран — Китая и России, являющихся одними из ведущих информационных государств.

В КНР первые шаги в области кибербезопасности были сделаны в 2006 году, когда была принята «Государственная стратегия по развитию информатизации на период с 2006 по 2020 г.». В ней изучены сферы, где могут возникнуть угрозы информационной безопасности; определены направления политики; предполагается создание собственного программного обеспечения. Также разрабатываются идеи мира и сотрудничества в информационной сети, идет «строительство информационной площадки для социализма с китайской спецификой». Согласно этой стратегии, все иностранные компании, связанные с IT, обязаны пройти сертификацию, чтобы работать на территории КНР. Власти Китая стремятся единолично контролировать информационное поле на своей территории, что подтверждается в Законе «О национальной безопасности» 2015 года. По нему зарубежные СМИ не могут публиковаться в стране без согласования со службами, а их информация не должна оппонировать официальным китайским новостным каналам[1].

Следующим шагом стал Закон о кибербезопасности КНР в 2016 году. Государство официально контролирует происходящее в сети Интернет: опубликованная там информация (в основном социальные сети) может храниться не дольше 6 месяцев, для любой онлайн

[1] Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. 2017. С. 159-160.

регистрации необходимы настоящие данные пользователя, контролируются виртуальные торговые сделки. При угрозе вводится ограничение к переписке, блокировка и запрет выхода в сеть[1]. С 2023 года планируется большая программа по безопасности данных, которая будет включать сотрудничество различных компаний, а также создание парков кибербезопасности[2].

В основном тенденции обеспечения кибербезопасности в КНР основываются на цензуре многих каналов с нежелательным для власти содержанием. С 2003 года реализуется программа «Золотой щит», которая блокирует сайты, противоречащие официальной политике Китая: например, где критикуется правительство. Все новости проходят фильтрацию. «Золотой щит» контролирует огромное количество сайтов и пользователей, аналога нет ни в одной другой стране. Еще одной программой является «Зеленая дамба», которая в основном защищает детей от порнографии и блокирует сайты, связанные с терроризмом. Из-за цензуры в КНР заблокированы многие международные сайты, поэтому были созданы свои аналоги[3].

Минусом такой закрытой системы можно назвать некую изолированность китайских граждан от всего мира, несмотря на незаконно проникающие крупицы внешней информации. К тому же, обеспечение кибербезопасности в больше направлено на защиту именно государства, тогда как отдельные граждане все еще подвержены риску, поскольку собираются их реальные данные, а китайские аналоги мессенджеров не обеспечены сильной системой шифрования.

Что касается государственных органов, обеспечивающих кибербезопасность, то главная роль здесь у военного аппарата, включающего в себя Военный совет ЦК КПК и Центральный военный

---

[1] Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. 2017. С. 159-160.

[2] Барковская А.А. Информационная безопасность в Китайской Народной Республике // Сборник статей студентов факультета права Белорусского государственного экономического университета. 2023. № 3. С. 33.

[3] Зверянская Л.П. Организационно-правовое обеспечение международной и национальной информационной безопасности: опыт Китайской Народной Республики // Труды Института государства и права РАН. 2017. Т. 12. № 5. С. 201-202.

совет КНР. В нем есть третий департамент, что разведывает деятельность в Интернете Китая и прорабатывает действия операций в сети. Важным звеном является Центральная комиссия по делам киберпространства, которая занимается вопросами цензуры и решает проблемы безопасности в Интернете[1].

Теперь рассмотрим Россию. В 2006 году был принят Федеральный закон «Об информации, информационных технологиях и о защите информации», который установил правила обработки информации. Стоит отметить, что в России многие правовые акты направлены на защиту и неприкосновенность именно личных данных граждан. В 2013 году подписан Указ Президента РФ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Создание данной системы было отдано Федеральной службе безопасности (ФСБ), которая еще должна проработать способы обнаружения кибератак и методику обмена информации между исполнительной властью об случившихся инцидентах, а также проводить мероприятия по оцениванию уровня защищенности инфраструктуры. Через год была принята концепция с идентичным названием, представляющая собой совокупность средств по обнаружению, предупреждению и ликвидации кибератак[2].

Следующим шагом в сфере кибербезопасности стал Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» 2017 года. Субъекты критической информационной инфраструктуры должны реагировать на события в цифровой сфере и принимать меры по ликвидации последствий совершенных киберпреступлений. Этот нормативный акт

[1] Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. 2017. С. 161-162.

[2] Лобач Д.В., Смирнова Е.А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2019. Т. 11. № 4. С. 27-29.

направлен на предупреждение кибератак и безопасность государственных и бизнес-структур[1].

Также в России проводятся аудиты информационных систем и устройств, чтобы найти уязвимые детали и устранить их до того, как ими воспользуются злоумышленники. Что касается связи, то с 2021 года ответственные за сервис должны обеспечить безопасность средств для пользователей от нежелательного доступа, дать информацию о защите устройств, а также исполнять требования к шифрованию данных и использовать российское программное обеспечение[2].

В нашей стране достаточно много ресурсов уделяется обучению населения противодействовать киберпреступлениям. Увеличиваются возможности поступить в высшее учебное заведение на специальности, связанные с информацией и современными технологиями: в некоторых университетах доступны направления, напрямую связанные с кибербезопасностью[3].

Минусом российской системы является «плавающая» формулировка кибербезопасности и принятых законов, которым не хватает конкретики. Роль государства в этой области достаточна мала, возникает необходимость укрепить сотрудничество власти с другими организациями для совместной защиты данных.

К государственным органам, которые отвечают за обеспечение кибербезопасности, в первую очередь относится Федеральный центр кибербезопасности при ФСБ, занимающийся защитой систем государства и проведением мероприятий по выявлению и предотвращению возможных атак. За обеспечение также отвечает МВД и Роскомнадзор. Последний следит за публикациями в сети Интернет

---

[1] Лобач Д.В., Смирнова Е.А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2019. Т. 11. № 4. С. 27-29.

[2] Забайкин Ю.В., Лунькин Д.А. Правовой аспект кибербезопасности и IoT в России // Вопросы Российского и международного права. 2023. Т. 13. № 121. С. 202.

[3] Там же.

и блокирует сайты и приложения, нарушающие российское законодательство.

Подводя итоги, можно отметить, что обе правовые системы — и Китая, и России — по обеспечению кибербезопасности функционируют и защищают сервисы и данные граждан и государства. В КНР достаточно жесткая система, контролирующая киберпространство страны и не пускающая в полном объеме иностранную информацию; тогда как в России сохраняется определенная свобода информации. К тому же в Китае следует направить силы по защите личных данных самих граждан. У РФ проблема заключается в нечеткой системе законодательства, а также в недостатке IT-специалистов, несмотря на увеличение мест в университетах. У Китая Россия могла бы подчерпнуть идею программы «Зеленая дамба». В целом обеим странам также стоит развивать международное сотрудничество, поскольку киберпреступления становятся глобальной проблемой.

СПИСОК ЛИТЕРАТУРЫ

1. Барковская А.А. Информационная безопасность в Китайской Народной Республике // Сборник статей студентов факультета права Белорусского государственного экономического университета. — 2023. — № 3. — С. 32-35.
2. Забайкин Ю.В., Лунькин Д.А. Правовой аспект кибербезопасности и IoT в России // Вопросы Российского и международного права. — 2023. — Т. 13, № 121. — С. 200-207.
3. Зверянская Л.П. Организационно-правовое обеспечение международной и национальной информационной безопасности: опыт Китайской Народной Республики // Труды Института государства и права РАН. — 2017. — Т. 12, № 5. — С. 196-214.
4. Лобач Д.В., Смирнова Е.А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. — 2019. — Т. 11, № 4. — С. 23-32.
5. Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. — 2017. — С. 156-170.