**Сравнение нормативно-правовых баз обеспечения кибербезопасности в России и Китае**

***Моисеева Ольга Владимировна***

*Студентка, 3 курс бакалавриата*

*Московский государственный университет имени М.В.Ломоносова,*

*Институт стран Азии и Африки, Москва, Россия*

*E–mail: moiseevao04@mail.ru*

В 2023 году во всем мире кибератаки совершались каждые 39 секунд. По прогнозам экспертов, их количество будет расти в 2024 году. Поэтому Россия и Китай, будучи крупными акторами на международной арене, рассматривают обеспечение кибербезопасности в качестве одного из приоритетных направлений внутренней и внешней политики. Законодательные акты, которые регулируют деятельность государства в данной сфере, должны изменяться по мере развития технологий, а также необходимо создавать новые органы по контролю за соблюдением данных законов. Скорость и характер реагирования государства на новый вид угроз является важным показателем уровня развития страны.

Хотелось бы отметить сложившуюся в международной практике разницу понятий «информационная безопасность» и «кибербезопасность». Термин «информационная безопасность» означает безопасность данных на любых носителях: электронных и традиционных (например, бумага, фотопленка, аудиокассеты). Кибербезопасность же ограничивается киберпространством, то есть защитой данных в электронной форме. Определение понятия «кибербезопасность» закреплено в Законе «О кибербезопасности» КНР [中华人民共和国网络安全法, 第七章]. Однако в российском законодательстве на данный момент не существует точного определения этого понятия.

Формирование законодательства по информационной безопасности началось в КНР раньше, чем в России. В КНР уже в 1994 году было опубликовано положение о безопасности и защищённости компьютерных информационных систем. Российское законодательство в данной сфере формировалось в 2000-х годах. Особый прорыв в расширении законодательства по информационной безопасности наблюдался в обеих странах в 2020-2023 годах: в Китае вступили в силу законы «О защите персональных данных» [中华人民共和国个人信息保护法], «О защите данных», в России вносились изменения в федеральные законы «Об информации, информационных технологиях и о защите информации» [ФЗ от 27.07.2006 N 149-ФЗ] и «О персональных данных» [ФЗ от 27.07.2006 N 152-ФЗ]. Одной из причин этого стала пандемия COVID-19, которая дала новые возможности для киберпреступников, поскольку все сферы жизни общества перешли в режим онлайн. Кроме того, число кибератак на российские структуры и компании увеличилось после начала Специальной военной операции, из-за чего потребовалось усиление системы защиты от подобных угроз.

Регулированием интернет-пространства и контролем над соблюдением законов в КНР занимается Государственная канцелярия интернет-информации, подконтрольная КПК и состоящая из Государственного информационного бюро Интернета и Центральной комиссии по делам киберпространства. Кроме того, в стране учреждено Министерство промышленности и информационных технологий, одной из функций которого является выдача специальной лицензии веб-сайтам для их работы. Например, компания Google не смогла получить данную лицензию, из-за чего сайт недоступен на территории КНР. Схожие функции в РФ выполняет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Данная служба подведомственна Министерству цифрового развития, связи и коммуникации (Минцифры) – основному органу по выработке государственной политики и нормативно-правовому регулированию в сфере информационных технологий. В центральный аппарат Минцифры также входит Департамент обеспечения кибербезопасности, схожий по функциям с Комиссией по делам киберпространства КНР.

О дальнейшем планировании развития системы кибербезопасности можно говорить на основе стратегий, публикуемых правительствами стран. В Китае в 2016 году была опубликована Национальная стратегия безопасности киберпространства [Горян, 2021, с. 117]. В России специализированной стратегии по данному вопросу нет. Ее проект разрабатывался еще в 2014 году, но так и не был принят. Однако не малое значение информационной безопасности придается в Концепции внешней политики Российской Федерации 2023 года и в Стратегии национальной безопасности Российской Федерации 2021 года [Указ Президента РФ от 02.07.2021 г. № 400, ст.48-57]. Термины кибербезопасность и киберпространство в указе Президента РФ не встречаются.

Таким образом, и Российская Федерация, и Китайская Народная Республика активно совершенствуют системы обеспечения кибербезопасности, оперативно реагируя на геополитические события в мире. И тем не менее, обе страны входят в десятку государств, подвергающихся наибольшему количеству кибератак, поэтому им необходимо расширять нормативно-правовую базу по этому вопросу и совершенствовать работу специальных органов.

**Источники и литература**

1. Указ Президента Российской Федерации от 02.07.2021 г. № 400 О Стратегии национальной безопасности Российской Федерации // Президент России URL: http://www.kremlin.ru (дата обращения: 27.02.2024)

2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ.

3. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ.

4. 中华人民共和国个人信息保护法 *//* 中华人民共和国中央人民政府URL: https://www.gov.cn (дата обращения: 28.02.2024).

5. 中华人民共和国网络安全法 *//* 中华人民共和国中央人民政府URL: https://www.gov.cn (дата обращения: 28.02.2024).

6. Горян Э.В. Нормативно-правовая основа обеспечения национальной безопасности в киберпространстве: опыт Китайской Народной Республики // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2021. – Т.13, №1. – с.115-124.