**А. Р. Богданова,**
аспирант,
Казанский инновационный университет
имени В. Г. Тимирясова

# РОЛЬ ГОСУДАРСТВА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

**Аннотация.** В статье анализируется роль государства в обеспечении безопасности критической информационной структуры. Обосновывается важность и актуальность обеспечения подобной защиты и участия государства в управлении. Кратко описаны основные функции государства и стратегии обеспечения защиты. Подчеркивается общая концепция национальной безопасности в качестве основной темы по обеспечению информационной безопасности. Автор делает вывод, что государство играет важнейшую роль в обеспечении безопасности критической информационной инфраструктуры, поскольку государство разрабатывает основные концепции обеспечения защиты и контролирует их.

**Ключевые слова:** кибербезопасность, государство, критическая информационная инфраструктура, национальная безопасность

The article analyzes the role of the state in ensuring the security of the critical information structure. The importance and relevance of ensuring such protection and state participation in management are substantiated. The main functions of the state and strategies for ensuring protection are briefly described. The article presents the main goals and ideals of ensuring the protection of the Russian Federation and China. The article emphasizes the general concept of national security as the main concept for ensuring information security. The author concludes that the state plays a vital role in ensuring the security of the critical information infrastructure, since the state develops the main concepts of the direction of ensuring protection and controls them.

K**eywords:** cybersecurity, state, critical information infrastructure, national security

Вопросы обеспечения национальной безопасности в целом, и обеспечение непосредственно информационной безопасности, в частности, являются ведущими направлениями деятельности на современном этапе развития государства [1].

Национальная безопасность является предпосылкой национального развития. Так, например, Китайская Народная Республика (далее – КНР), крайне обеспокоена обеспечением кибербезопасности, так как 14-й пятилетний план и план развития до 2035 года рассматривают «координацию развития и безопасности и построение более безопасного Китая на более высоком уровне» как важную руководящую идеологию, расширяя горизонты и теории исследования управления рисками безопасности [2]. Безопасность критической информационной инфраструктуры (далее – КИИ) связана с национальной экономикой и жизнедеятель-

ностью людей. Она играет важную роль для национальной экономики и жизнедеятельностью людей в разных сферах [3].

КИИ является важным краеугольным камнем, поддерживающим функционирование страны и общества, охватывая многие отрасли и сферы. Поэтому обеспечение безопасности КИИ является важной гарантией поддержания национальной безопасности и социальной стабильности. Генеральный председатель КНР Си Цзиньпин подчеркивает, что КИИ в сфере финансов, энергетики, электроснабжения, связи и транспорта требует обеспечения крайне высокого уровня безопасности [4].

Государства в целях обеспечения безопасности КИИ разрабатывают различные нормативные правовые акты, которые обеспечивают прочную правовую основу для развития этого института. Эти акты определяют сферу действия КИИ, принципы защиты, систему надзора и управления, обязанности операторов, формулируют меры безопасности, а также устанавливают юридическую ответственность, закладывая прочную правовую основу для всех сторон. Законодательство государств о защите КИИ закрепляют наиважнейшие принципы управления такими объектами, защиту информации, обеспечение устойчивости КИИ в целом и ее отдельных элементов, а также управление кризисами и чрезвычайными ситуациями [5].

Страны обеспечивают создание систем и механизмов управления для защиты КИИ, подробно определяющих роли национальных ведомств и органов по обеспечению кибербезопасности. Государства регулируют создание механизмов обмена информацией, координирует обмен информацией о состоянии обеспечения кибербезопасности между ведомствами, координирует соответствующие департаменты и органы для создания механизма реагирования между соответствующими департаментами, департаментами защиты, операторами и службами по кибербезопасности.

Государства поощряют и поддерживают инновации в области технологий кибербезопасности для повышения эффективности сетевой защиты. Важно отметить также роль государства в усилении надзора и контроле правоприменения. Так, соответствующие национальные ведомства обеспечивают надзор и контроль правоприменения в отношении КИИ и обеспечивают профилактику нарушений законодательства.

Таким образом, можно сказать, что государство посредством политического воздействия, финансовой поддержки и других мер, играет незаменимую роль в обеспечении безопасности КИИ. Именно государство предоставляет надежные гарантии обеспечения безопасности КИИ путем разработки нормативных правовых актов, создания систем и механизмов управления, предоставления технической поддержки, усиления надзора и управления, проведения проверок систем безопасности, а также содействия инновациям в области технологий защиты безопасности и промышленного развития. И, если государство продолжит расширять возможности независимых инноваций, укреплять механизмы мониторинга рисков безопасности и раннего оповещения, а также укреплять международное сотрудничество и обмены для всестороннего повышения уровня защиты КИИ, это поможет обеспечить безопасную и стабильную работу КИИ, окажет

мощную поддержку экономическому и социальному развитию, а также будет способствовать повышению статуса и влияния самой страны в сфере международной кибербезопасности.

## Список литературы

1. Горохова С.С. О некоторых аспектах обеспечения безопасности критической информационной инфраструктуры в Российской Федерации // Право и политика. 2018. № 6.

2. 王驰，曹劲松.数字新型基础设施建设下的安全风险及 其治理[J].江苏社会科学，2021，318(05):88-99+242-243. Ван Чи, Цао Цзиньсун. Риски безопасности и управление при создании новой цифровой инфраструктуры [J]. Jiangsu Social Sciences, 2021, 318(05):88-99+242-243.

3. 张艺腾.总体国家安全观视域下的关键信息基础设施 安全防护[J].网络安全技术与应用，2023，267(03):158-160. Чжан Итэн. Защита безопасности критической информационной инфраструктуры с точки зрения общей национальной безопасности [J]. Технологии и приложения сетевой безопасности, 2023, 267(03):158-160.

4. 中共中央党史和文献研究院.论党的宣传思想工作[M].北京:中央文献出版社，2020. Научно-исследовательский институт истории партии и литературы при ЦК КПК. О пропагандистской и идеологической работе партии[M]. Пекин: Центральное литературное издательство, 2020.

5. Jangirala, Srinivas & Das, Ashok Kumar & Kumar, Neeraj. (2018). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems. 92. 10.1016/j.future.2018.09.063.