***В.В. Хоружий,***

*Магистрант 1 курса*

*Направление 40.04.01 «Юриспруденция»*

*ФГБОУ ВО Кубанский ГАУ имени И.Т. Трубилина,*

*г. Краснодар*

**КИБЕРБЕЗОПАСНОСТЬ В РФ: НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ**

**CYBERSECURITY IN THE RUSSIAN FEDERATION: LEGAL REGULATION**

**Аннотация:** статья посвящена вопросам нормативно-правового регулирования обеспечения кибербезопасности. Проведен анализ потенциальных путей развития нормативной базы. Предложены общие направления государственного регулирования в обеспечении кибербезопасности.

**Ключевые слова:**кибербезопасность, киберпространство, киберпреступления, информационная безопасность.

**Annotation:** the article is devoted to legal regulation of cybersecurity. The analysis of potential ways of development of the regulatory framework. Proposed General directions of state regulation in cybersecurity

**Keywords**: cybersecurity, cyberspace, cyber crimes, information security.

Термин «кибербезопасность» все чаще встречается в научном дискурсе современной России. Серьёзность отношения к проблеме кибербезопасности определена глобальными вызовами и локальными изменениями внутри страны, что заставляет российское законодательство реагировать и принимать меры. В условиях существования современного информационного общества национальная безопасность любой страны напрямую зависит от безопасности информационных систем.

Нельзя не согласиться с тем, что задача нормативно-правового регулирования обеспечения кибербезопасности является одним из важнейших компонентов государственной политики развития национального сектора применения информационных технологий [1]. Причин для этого в наше неспокойном времени много, ведь информационные ресурсы стали сейчас полем брани на всех уровнях: физическом, цифровом, институциональном. Можно привести множества таких негативных примеров: от взлома аккаунта социальных сетей Министерства обороны США до глобальной кибератаки с использованием так называемого вируса-вымогателя, который в мае 2017 года затронул более 200 тысяч пользователей в 150 странах.

Необходимо учитывать, что существует несколько уровней указанной проблемы: от частного, связанного с защитой граждан и конкретного человека, от злоумышленников разного рода до государственного и надгосударственного, где решаются задачи национальной безопасности и информационных войн.

На сегодняшний день к нормативно-правовым документам, обеспечивающим кибербезопасность можно отнести:

- Закон Российской Федерации от 27.07.2006 № и149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года»;

- Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

- Указ Президента Российской Федерации от [5 декабря 2016 года № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».](http://www.consultant.ru/document/Cons_doc_LAW_208191/)   
 Указанные документы закладывают основу для совершенствования правового регулирования обеспечения кибербезопасности. Но остаются нерешенными многие вопросы теоретического и организационного характера.

«Правовое регулирование не охватывает всего сложившегося многообразия отношений, возникающих в рамках киберпространства. Анализ показывает, что в официальных российских документах в области информационной безопасности термин «кибербезопасность» не используется отдельно» [2, с. 1695].

Сегодня в России нет единой концепции стратегии кибербезопасности. Разрабатываемый специальной комиссией Совета Федерации проект такой стратегии, которая могла бы заложить основы правового взаимодействия всех участников киберпространства, так и остался несогласованным.

Между тем, количество киберпреступлений растет как в России, так и во всем мире. По данным информационно-правового портала ГАРАНТ.РУ на Россию в 2012 году пришлось 20% киберпреступлений в мире [3].

Необходимость координации взаимодействий в правовой сфере подчеркивают руководители высшего ранга. В июне 2017 года на экспертном форуме «Примаковские чтения» глава МИД РФ Сергей Лавров в ходе своего выступления подчеркнул: «Особую тревогу вызывает масштабный рост киберпреступности, участившиеся использование информационных и коммуникационных технологий в целях оказания воздействия на общественно-политическую и социально-экономическую обстановку» [4]. Лавров отметил, что Россия долгие годы добивается принятия под эгидой ООН правил поведения государств в киберпространстве и ждет ответа от западных коллег.

В целях дальнейшего совершенствования обеспечения кибербезопасности государству необходимо вести постоянный мониторинг киберугроз, профилактику кибертерроризма, развивать навыки кибербезопасности, стимулировать научные исследования в сфере кибербезопасности и совершенствовать нормативно-правовую базу для регулирования взаимодействий в киберпространстве.

**Список использованной литературы:**

[1]. Матвеев, В.А. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации / В.А. Матвеев, В.Л. Цирлов // Вопросы кибербезопасности. – 2013. – № 1(1). – С. 61 - 64.

[2]. Суханов, А.Г. Особенности правового регулирования в области обеспечения кибербезопасности критической инфраструктуры / А.Г. Суханов // Экономика и социум. – 2017. – № 3(34). – С. 1693 - 1700.

[3]. Михайлова, А. Проблемы кибербезопасности в России и пути их решения[Электронный ресурс] – Режим доступа: <http://www.garant.ru/article/520694/> – Загл. с экрана. (Дата обращения 04.05.2020 г.)

[4]. Россия ожидает от Запада ответ на предложения по кибербезопасности [Электронный ресурс] – Режим доступа: <https://riafan.ru/846858-rossiya-ozhidaet-ot-zapada-otvet-na-predlozheniya-po-kiberbezopasnosti-lavrov> – Загл. с экрана. (Дата обращения 04.05.2020 г.)

*© В.В. Хоружий, 2020*