Гаджиев Г.К. Правовые аспекты защиты информации: сравнительный анализ законодательства разных стран в области кибербезопасности// Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 4(54) с. 38–41

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА РАЗНЫХ СТРАН В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Гаджиев Г.К.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: gugac134@gmail.com

В статье проводится сравнительный анализ законодательства различных стран в области кибербезопасности. Рассматриваются ключевые нормативные акты, регулирующие защиту информации, а также подходы к предотвращению и расследованию киберпреступлений. Особое внимание уделяется различиям в правовых системах США, Европейского Союза, России и Китая, а также их влиянию на глобальную политику информационной безопасности. Проанализированы тенденции развития законодательной базы и предложены рекомендации по унификации международных стандартов защиты данных.

Ключевые слова: Кибербезопасность, законодательство, защита информации, киберпреступления, нормативные акты, международное право, персональные данные.

LEGAL ASPECTS OF INFORMATION PROTECTION: A COMPARATIVE ANALYSIS OF THE LEGISLATION OF DIFFERENT COUNTRIES IN THE FIELD OF CYBERSECURITY

Gadzhiev G.K.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: gugac134@gmail.com

The article provides a comparative analysis of the legislation of different countries in the field of cybersecurity. The key regulations governing information security, as well as approaches to the prevention and investigation of cybercrimes, are considered. Special attention is paid to the differences in the legal systems of the United States, the European Union, Russia and China, as well as their impact on global information security policy. The trends in the development of the legislative framework are analyzed and recommendations for the unification of international data protection standards are proposed.

Keywords: Cybersecurity, legislation, information protection, cybercrime, regulations, international law, personal data.

Введение

С развитием цифровых технологий и ростом числа киберугроз защита информации становится одной из ключевых задач государств. В различных странах разработаны собственные нормативные акты, регулирующие вопросы кибербезопасности, однако их содержание и принципы значительно различаются. В данной статье проводится сравнительный анализ законодательных подходов к защите информации в разных юрисдикциях, с акцентом на нормативные акты США, Европейского Союза, России и Китая.

Изучение правовых аспектов кибербезопасности позволяет выявить сильные и слабые стороны национальных стратегий и определить перспективы международного сотрудничества [1-2].

Законодательство США в области кибербезопасности. В Соединённых Штатах вопросы защиты информации регулируются несколькими основными законами, такими как Закон о модернизации кибербезопасности (CISA), Закон о защите критической инфраструктуры (CIP) и Закон о компьютерном мошенничестве и злоупотреблениях (CFAA). Эти акты направлены на предотвращение кибератак, защиту персональных данных и координацию взаимодействия между государственными органами и частным сектором. Важной особенностью американского законодательства является наличие отдельных законов для различных отраслей экономики, например, HIPAA для здравоохранения и GLBA для финансового сектора[3].

Регулирование кибербезопасности в Европейском Союзе. Европейский Союз реализует комплексный подход к защите данных, основными документами которого являются Общий регламент по защите данных (GDPR) и Директива NIS (Network and Information Security). GDPR устанавливает строгие требования к обработке персональных данных и предусматривает серьёзные штрафы за их нарушение. Директива NIS фокусируется на обеспечении безопасности критической инфраструктуры и цифровых сервисов. В отличие от США, законодательство ЕС делает акцент на защите прав пользователей и прозрачности обработки данных.

Кибербезопасность в законодательстве России. В России нормативная база в области защиты информации представлена Федеральным законом "О безопасности критической информационной инфраструктуры Российской Федерации", Законом "О персональных данных" и рядом подзаконных актов. Российское законодательство ориентировано на защиту национальных интересов и суверенитет в цифровой сфере. Важное место занимает регулирование деятельности иностранных IT-компаний, в том числе требования о локализации данных российских граждан [4].

Кибербезопасность в Китае. Китайская система регулирования кибербезопасности является одной из самых жёстких в мире. Основным нормативным актом является Закон КНР о кибербезопасности, который устанавливает строгие требования к защите данных, мониторингу интернет-активности и контролю за деятельностью иностранных технологических компаний. Китайская политика в данной сфере направлена на обеспечение национальной безопасности и защиту государственных интересов в киберпространстве.

Сравнительный анализ и перспективы международного сотрудничества. Сравнение законодательных систем разных стран показывает значительные различия в подходах к регулированию кибербезопасности. США ориентированы на защиту бизнеса и развитие инноваций, ЕС делает акцент на права пользователей, Россия и Китай придерживаются модели цифрового суверенитета. Эти различия создают препятствия для международного сотрудничества, однако необходимость борьбы с глобальными киберугрозами требует

формирования единых стандартов. В этом контексте перспективными направлениями являются разработка международных соглашений по обмену информацией, согласование требований к обработке данных и унификация мер реагирования на кибератаки.

Заключение.

Правовое регулирование кибербезопасности играет ключевую роль в обеспечении защиты данных и цифровых систем. Анализ законодательства США, ЕС, России и Китая демонстрирует различные подходы к решению данной проблемы, обусловленные национальными интересами и политическими приоритетами. Несмотря на существующие различия, развитие международного сотрудничества и унификация стандартов безопасности являются необходимыми шагами для эффективной борьбы с киберугрозами в глобальном масштабе.

Список литературы

1. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 563-568.
2. Кирилова К. С. и др. Проблема обезвреживания руткитов уровня ядрав системах специального назначения //I-methods. – 2020. – Т. 12. – №. 3. – С. 2.
3. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76].
4. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 570-573.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 63 с. – EDN CMMEML.

References

1. Katasonov A. I., Tsvetkov A. Yu. Analysis of access control mechanisms in special-purpose systems // Actual problems of infotelecommunications in science and education (APINO 2020). - 2020. - pp.563-568.
2. Kirilova K. S. et al. The problem of neutralizing kernel-level rootkits in special-purpose systems // I-methods. - 2020. - Vol. 12. - No. 3. - p. 2.
3. Pestov I. E. Methodology for developing control action on cloud infrastructure instances // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. - No. 4. - pp.72-76.
4. Suvorov A. M., Tsvetkov A. Yu. Study of buffer overflow attacks in 64-bit unix-like operating systems // Actual problems of infotelecommunications in science and education (APINO 2018). - 2018. - pp. 570-573.

5. Shterenberg, S. I. Computer viruses / S. I. Shterenberg, A. V. Krasov, A. Yu. Tsvetkov. Volume Part 1. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2015. - p. 63 - EDN CMMEML.