УДК:004.056

Белов И.А.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

Научный руководитель:
Новикова Д.Д.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

ПОЛИТИКА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ, США, КИТАЕ И ЕС

Аннотация. Статья посвящена анализу политики в сфере информационной безопасности в России, США, Китайской Народной Республике и Европейском Союзе. В работе рассматриваются различные подходы этих стран к обеспечению кибербезопасности, а также выявляются как положительные, так и отрицательные аспекты их политик. В результате проведенного анализа сделан вывод о том, что эффективная стратегия в области информационной безопасности должна находить оптимальный баланс между обеспечением безопасности и развитием международного сотрудничества.

Ключевые слова: информационная безопасность, информационная политика, Интернет, киберпространство.

Одна из притч мудрого царя Соломона звучит так: «Благоразумный видит беду, и укрывается; а неопытные идут вперед, и наказываются». В век информационных технологий эта притча очень актуальна.

Современные угрозы в цифровом пространстве становятся сложными и разнообразными, что требует значительных усилий для поддержания кибербезопасности.

В разных странах мира их собственные стратегии создаются для формирования информационной безопасности [2]. Рассмотрим примеры такой политики в России, Китае, США и Европейском союзе.

Наша страна нацелена на формирование национальной цифровой среды, включая свои системы поиска, социальные сети и услуги обмена сообщениями. К 2021 г. введен в действие Закон «суверенного Интернета», содержащий положения создать национальную систему управления интернет-трафиками, регулируя ключевые информационные ресурсы. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 определил список предметов квот и установил требования для их защиты. Недавний Указ 13 июня 2024 г. № 500 обновил ряд положений. Согласно новому правилу, в 2025 г. государственным структурам и предприятиям запрещено использовать инструменты защиты информации, разработанные компаниями из стран в состоянии недружелюбных связей. Федеральной службе безопасности в России теперь назначено право определять условия работы с центрами, включенными в систему защиты [1]. План стратегического развития для российской ИТ промышленности за период с 2024 по 2030 г. сконцентрирован на поддержание технологической независимости цифровой техники. Сформирован Национальный координационный центр компьютерных мероприятий (NKSKI). С 2019 г. «Цифровой диктант» организуется регулярно Российской Ассоциацией электронных коммуникаций (РАЭК). Данный диктант состоит из тестирований, которое разработано с учетом разных возрастных категорий: для детей (7–13 лет), подростков (14–17 лет), взрослых (18–59 лет). Онлайн-платформа «Цифровой гражданин», действующая с 2018 г., предлагает учебные ресурсы и проводит сертификацию сотрудников в государственных и торговых организациях. 30 ноября 2024 г. Президент Российской Федерации подписал законнодательные действия, направленные на привлечение как к административной, так и уголовной ответственности за нарушение Российского Законодательства по личным сведениям [6]. Федеральный закон № 420, который меняет Кодекс административных преступлений, был принят 3 ноября 2024 г. Федеральный закон № 421 от 30 ноября 2024 г. вводит специальный корпус Delicti в Уголовный кодекс Российской Федерации по контрактам на личную информацию, имеет силу с 11 декабря 2024 г. [5].

Среди компаний, сосредотачивающих свою деятельность на кибербезопасности, «Лаборатория Касперского», конечно, занимает лидирующие положения в России. Softline, московская компания,

находится на «ступеньке ниже» по объему выручки и предоставляет просторный спектр ИТ-сервисов, включая решения для киберзащиты. Вслед за ними идут такие компании, как BI.Zone Cybersecurity, GIS, Solar и Positron. С целью улучшения уровня защиты от киберугроз, я думаю, необходимо сотрудничество между СМИ, государственными органами и бизнесом. Минцифры разрабатывает платформу «ТелекомЦерт». Старт этой разработки намечен на конец 2026 г. [5].

Квантовые компьютеры, действительно, представляют собой потенциальную угрозу безопасности информации. В России ведутся экспериментальные разработки по внедрению постквантового шифрования, осуществляемые структурным подразделением «Российского квантового центра» [4].

Безопасность информации в США ориентирована, в первую очередь, на независимость всемирной сети и небольшое государственное вмешательство. Отражено это в законодательстве, включая CLOUD Act (2018). В 2019 г. был введен запрет на применение федеральных средств с целью закупки оборудования и услугу Huawei и ZTE. США заставляют союзников отказываться от оборудования в сетях 5G. Изданный Указ президента США № 14028 «Об усилении кибербезопасности страны» (2021) содержит 74 директивы, устанавливающие общие правила взаимодействия с кибератаками между федеральными агентствами и коммерческими организациями. Незащищенности в программном обеспечении Microsoft и Atlassian использовались, чтобы похитить сети. AWS занимает лидирующие положения в США и союзных государствах в плане сохранности и обработки секретной информации.

Китайская политика, в первую очередь, базируется на концепции и киберсуверенитета, подразумевающей надзор государства над глобальной сетью. Китай активно контролирует интернет, сдерживая иностранные ресурсы, и развивает свои компьютерные методики, такие как Baidu и WeChat, для уменьшения подчиненности от западных технологий. Вопреки всему, Китай не стремится к изоляции. Взгляды Российской Федерации и Китая на кибербезопасность в большинстве вопросов совпадают.

Европейский союз (ЕС) стремится к защите цифровых прав граждан, а также уменьшению влияния китайских технологий. Цифровой суверенитет в ЕС связан с защитой персональных данных, а отражено это в Общем регламенте по защите данных (GDPR), устанавливающем высокие стандарты защиты данных. ЕС также достигает совершенства своей цифровой инфраструктуры в рамках стратегии «Формирование цифрового будущего Европы», включая создание облачного хранилища Gaia-X. Главной частью системы кибербезопасности ЕС является Вторая директива о сетях и информационных системах (NIS2), обязывающая государства разрабатывать стратегии кибербезопасности.

Таблица 1

Преимущества и недостатки в деятельности политики ИБ

Страны	Преимущества	Недостатки
Россия	Независимость от западных технологий и устойчивость к атакам	Ограничение конкуренции
США	Собственное технологическое развитие и отстаивание национальных интересов	Высокая стоимость разработки и внедрения
Китай	Быстрое развитие собственных цифровых технологий и платформ	Высокие барьеры для выхода иностранных компаний на китайский рынок
ЕС	Высокий уровень защиты персональных данных граждан и мотивация усовершенствования европейской цифровой инфраструктуры	Немалая цена соблюдения GDPR для предпринима-тельства, а также ограничен-ность резервов и власти Европейского агентства по кибербезопасности

Таким образом, анализируя данные, пришли к следующим выводам:

1. Если ограничить системы телекоммуникаций стран, то при создании сетей будет иметь меньший результат по сравнению с обменом информации для усиления мер защиты.
2. Геополитическое соперничество имеет отношение и к гиперпространству.
3. Эффективная стратегия должна балансировать между безопасностью и сотрудничеством между странами.

Список использованных источников:

1. Указ Президента РФ от 13.06.2024 № 500 «О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"». URL: https://www.consultant.ru/law/hotdocs/85170.html.
2. Информационная безопасность. URL: https://ru.wikipedia.org/wiki.
3. На платформу становись. Минцифры поднимает отрасли на борьбу с киберугрозами. URL: https://www.kommersant.ru/doc/6905615, 21.08.2024.
4. НСПК и QApp реализовали пилот по защите данных на основе постквантовых алгоритмов шифрования. URL: https://safe.cnews.ru/news/line/2023-11-10_nspk_i_qapp_realizovali_pilot.
5. Степанова Г.А. Основные изменения в правовом обеспечении защиты информации, персональных данных и функционирования ИС в РФ в 2025 г. // Корпоративные информационные системы. 2024. № 4 (28). С. 1–9. URL: https://corpinfosys.ru/archive/2024/issue-28/259-2024-28-itlawschangesin2025.

6. Цифровой суверенитет как залог глобальной безопасности. URL: https://roscongress.org/materials/tsifrovoy-suverenitet-kak-zalog-globalnoy-bezopasnosti/.

Belov I.A.
Volga Region State University of
Telecommunications and Informatics, Samara

Scientific supervisor:
Novikova D.D.
Volga Region State University of
Telecommunications and Informatics, Samara

INFORMATION SECURITY POLICYIN RUSSIA, THE USA, CHINA A ND THE EU

Abstract. The article analyzes the policies in the field of information security in Russia, the United States, the People's Republic of China and the European Union. The work examines the various approaches of these countries to ensuring cybersecurity, and identifies both positive and negative aspects of their policies. As a result of the analysis, it is concluded that an effective strategy in the field of information security should find an optimal balance between ensuring security and developing international cooperation.

Keywords: information security, information policy, Internet, cyberspa.