4. МВФ: статистика по странам URL: https://www.imf.org/en/Countries
5. Уровень безработицы по странам URL: https://worldpopulationreview.com/country-rankings/unemployment-by-country
6. ВНП по странам URL: https://worldpopulationreview.com/country-rankings/gnp-by-country
7. Дальнейшее развитие ШОС на фоне новых реалий URL: https://eurasia.today/actual/dalneyshee-razvitie-shos-na-fone-novykh-realiy/

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

А.Ю. Мокшина
Науч. рук.: Г.С. Беляева
Белгород, Россия
Белгородский государственный
национальный исследовательский университет

Аннотация: *данная статья посвящена проблеме обеспечения информационной безопасности как одного из ключевых элементов системы национальной безопасности современного российского государства. Автором анализируются основные виды проблем, особое внимание уделяется вопросам недостаточной защищенности критической инфраструктуры, проблемам конфиденциальности персональных данных. Рассматриваются также трудности, связанные с распространением дезинформации. Предлагаются пути решения указанных проблем.*

Ключевые слова: *информационная безопасность, национальные приоритеты, информационные угрозы, информационная инфраструктура*

INFORMATION SECURITY ISSUES IN THE NATIONAL SECURITY SYSTEM OF THE RUSSIAN FEDERATION

A.Y. Mokschina
Scientific Supervisor: G.S. Belyaeva
Belgorod, Russia
Belgorod State National Research University

Abstract: *this article is devoted to the problem of ensuring information security as one of the key elements of the national security system of the modern Russian state. The author analyzes the main types of problems, paying special attention to the issues of insufficient security of critical infrastructure, and the problems of confidentiality of personal data. Difficulties associated with the spread of disinformation are also considered. Ways to solve these problems are proposed.*

Keywords: *information security, national priorities, information threats, information infrastructure*

Проведя сравнительный анализ Стратегий национальной безопасности 2015 [10] и 2021 [1] годов, можно заметить, что информационная безопасность, представленная в качестве одного из стратегических национальных приоритетов, появилась только в Стратегии 2021 года, расположена сразу после государственной и общественной безопасности, выше экономической.

Указом Президента РФ от 5 декабря 2016 г. № 646 была утверждена Доктрина информационной безопасности Российской Федерации. Согласно ей, под информационной безопасностью мы будем понимать «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [1].

Информационная безопасность имеет стратегическое значение, обеспечивая защиту интересов личности, общества и государства в информационном пространстве, представляя собой один из ключевых элементов национальной безопасности государства.

Современные угрозы информационной безопасности характеризуются комплексностью, то есть включают как внешние, так и внутренние факторы воздействия на информационную инфраструктуру страны.

Анализ проблем обеспечения информационной безопасности начнем с того, что несмотря на то, что в последние года особое внимание уделяется развитию критической информационной инфраструктуры нашей страны, она до сих пор остается уязвимой к кибератакам. Так, например, в июле 2025 года «Аэрофлот» подвергся масштабной кибератаке, парализовавшей работу авиакомпании, что привело к отмене рейсов и задержкам [2].

Второй немаловажной проблемой стала недостаточная конфиденциальность персональных данных пользователей, проблемы с уязвимостями в системах защиты, неправильной настройки серверов и систем хранения. Так, в марте 2022 года произошла массовая утечка данных пользователей «Яндекс.Еды». Она затронула адреса клиентов, номера телефонов, электронные почты и суммы заказов за последние полгода.

Также в качестве проблемы отметим, то, что хакеры очень быстро придумывают новые способы воздействия на нашу информационную систему. Так, например, хакеры начали атаковать российские компании через умные гаджеты. Согласно результатам исследования, которое провела RTM Group, хакеры стали получать доступ к конфиденциальной информации российских предприятий с помощью портативных колонок, зарядных станций и кружек с подогревом [3].

Особое внимание необходимо уделить развитию социальных сетей и мессенджеров. В последние два года участились случаи распространения ложной информации, в том числе такую информацию хакеры научились выдавать от лица официальных лиц государства. Например, в марте 2024 года была совершена хакерская атака на электронные сервисы официальных лиц Белгородской области, в результате распространяется ложное сообщение от лица губернатора региона Вячеслава Гладкова. В таких случаях необходимо помнить о том, что доверять можно только проверенным источникам информации и официальным аккаунтам государственных служащих [4].

Важно отметить, что хакерские атаки наносят большой ущерб экономике нашей страны. Так, по оценкам Сбербанка за первую половину 2025 года количество кибератак на российский бизнес увеличилось в три раза по сравнению с аналогичным периодом прошлого года. Ущерб экономике России за этот период может достигнуть ₽1,5 трлн. Зампред правления Сбербанка Станислав Кузнецов подчеркнул, что кибератаки все чаще нацелены на государственный сектор, что свидетельствует о недостаточном уровне киберзащиты в этих структурах. По данным Сбербанка, в 2025 году кибератакам подверглись не менее 53% российских компаний. Из них 80% столкнулись с серьезными последствиями, включая репутационные риски и финансовые потери. Примерно 48% компаний сообщили о простоях в работе [5].

В качестве одного из элементов механизма усовершенствования обеспечения информационной безопасности традиционно выделим, прежде всего, разработку и совершенствование нормативной правовой базы. Несмотря на то, что в нашей стране существует большое число специализированных актов в сфере информационной безопасности, на наш взгляд, недостаточно комплексного единого федерального закона, регулировавшего бы конкретно сферу обеспечения информационной безопасности. На данный момент правовая основа информационной безопасности строится, прежде всего на Конституции Российской Федерации (перечислены основные права граждан в информационной сфере, например, в ст. 42 устанавливается право на достоверную информацию о состоянии окружающей среды), также на специализированных федеральных законах: «Об информации, информационных технологиях и о защите информации», «О безопасности», «О коммерческой тайне», «О персональных данных» и др. Нельзя забывать и

о подзаконном правовом регулировании, здесь, прежде всего отметим, упомянутый выше Указ Президента РФ от 5 декабря 2016 г. № 646, которым была утверждена Доктрина информационной безопасности Российской Федерации, также Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и другие. Несмотря на то, что это далеко не все правовые акты регулирующие информационную сферу, все же необходим единый акт, обобщающий все положения, для исключения правовых коллизий и разночтений.

Важным инструментом обеспечения безопасности является навык быстрого реагирования и адаптация к постоянному развитию информационных угроз, необходимо создать надежные системы мониторинга и контроля за информационной сферой, например, с использованием искусственного интеллекта, создать возможность общественного контроля за информацией, в том числе в сети «Интернет».

Обучение и повышение квалификации сотрудников государственных органов, частных компаний и т.д. в сфере защиты информации. Современные технологии развиваются стремительно, а вместе с ними меняются и способы атак. Сотрудники должны регулярно обновлять знания и навыки, чтобы эффективно противостоять новым угрозам, особенно учитывая тот факт, что большинство утечек информации происходят именно из-за ошибок сотрудников.

Литература

1. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // СПС КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 13.10.2025)
2. Хакерская атака на «Аэрофлот»: кто стоит за киберсбоем в Шереметьево// ВФокусе Mail. – URL: https://vfokuse.mail.ru/article/hakerskaya-ataka-na-aeroflot-kto-stoit-za-kibersboem-v-sheremetevo-67209338/ (дата обращения: 13.10.2025)
3. Хакеры начали атаковать российские компании через кружки с подогревом // LENTA.RU. – URL: https://lenta.ru/news/2025/10/09/hakery-nachali-atakovat-rossiyskie-kompanii-cherez-kruzhki-s-podogrevom/ (дата обращения: 13.10.2025)
4. В Белгородской области назвали фейком оповещение от «губернатора» // NEWS.ru. – URL: https://news.ru/regions/v-belgorodskoj-oblasti-nazvali-fejkom-opoveshenie-ot-gubernatora?ysclid=mgrqoiws5e868574915 (дата обращения: 13.10.2025)
5. Кибератаки угрожают экономике РФ ущербом в ₽1,5 трлн // Новости Mail. – URL: https://finance.mail.ru/article/kiberataki-ugrozhayut-ekonomike-rf-uscherbom-v-1-5-trln-67740080/?ysclid=mhbltsl9s9843983415 (дата обращения: 13.10.2025)
6. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) // СПС КонсультантПлюс – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 13.10.2025)
7. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 04.08.2023) (с изм. и доп., вступ. в силу с 05.08.2024) // СПС КонсультантПлюс – URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 13.10.2025)
8. Беляева, Г.С. Правовое регулирование информационной безопасности: учебное пособие / Г.С. Беляева, Н.В. Бородаенко, Ю.А. Комнатная. – Белгород: ИД «Белгород» НИУ «БелГУ», 2024. – 80 с.
9. Ланецкая А.Ю., Александрова Е.Н. Современные угрозы информационной безопасности // Международный журнал гуманитарных и естественных наук. – 2022. – №7-2. – С. 192-195.
10. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31.12.2015 № 683 // СПС КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_191669/ (дата обращения: 13.10.2025)