ПУБЛИЧНО-ПРАВОВЫЕ ИССЛЕДОВАНИЯ

УДК 34:006.015.8
ББК 67.401.114

АКТУАЛЬНЫЕ ВЫЗОВЫ И УГРОЗЫ ИНФОРМЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОМ ОБЩЕСТВЕ И ПРАВЕ XXI В.

И. А. Воронина, А. В. Кирпичникова
Оренбургский государственный университет (Оренбург, Россия)

В статье рассматриваются динамичные изменения в сфере информационной безопасности, с которыми сталкивается Российская Федерация на современном этапе, а также анализируются ключевые факторы, формирующие ландшафт угроз в XXI в., включая стремительную цифровую трансформацию, геополитическую напряженность и эволюцию киберпреступности. Выделяются и подробно характеризуются категории угроз: технологические, социально-психологические, геополитические и экономические. Особое внимание уделено роли российского права в обеспечении информационной безопасности, характеристике существующих законодательных актов и вызовам в их практическом применении и предлагаются направления для дальнейшего совершенствования системы защиты.

Ключевые слова: информация, цифровизация, информационная безопасность, право, общество

CURRENT CHALLENGES AND THREATS TO INFORMATION SECURITY IN RUSSIAN SOCIETY AND LAW OF THE 21ST CENTURY

I. A. Voronina, A. V. Kirpichnikova
Orenburg State University (Orenburg, Rassia)

The article examines the dynamic changes in the field of information security faced by the Russian Federation at the present stage, as well as analyzes the key factors shaping the threat landscape in the 21st century, including rapid digital transformation, geopolitical tensions and the evolution of cybercrime. The categories of threats are highlighted and characterized in detail: technological, socio-psychological, geopolitical and economic. Special attention is paid to the role of Russian law in ensuring information security, the characteristics of existing legislative acts and challenges in their practical application, and the directions for further improvement of the protection system are proposed.

Keywords: information, digitalization, information security, law, society

Doi: https://doi.org/10.14258/ralj(2025)3.5

На рубеже XX–XXI вв. человечество вступило в эпоху глобальной цифровой трансформации, которая кардинально изменила характер социально-экономических, политических и культурных взаимодействий. Российская Федерация, являясь активным участником этого процесса, не только осваивает преимущества цифровизации, но и сталкивается с беспрецедентным спектром вызовов и угроз в информационном пространстве [7, с. 119]. В связи с чем информационная безопасность перестала быть узкотехнической проблемой, превратившись в один из ключевых факторов национальной безопасности, суверенитета и устойчивого развития.

Информатизация, цифровизация и информационные технологии очень прочно интегрируются в повседневную реальность, порождая рост проблемы обеспечения информационной безопасности в масштабах государства. В данном случае актуальной видится оперативная реакция законодателя на вызовы, угрожающие информационной безопасности, конечно, с учетом национальных интересов и стратегии. Современный контекст характеризуется не только усложнением технологической среды, но и обострением геополитических противоречий, переносом многих форм противоборства в киберпространство. В этих условиях понимание, классификация и эффективное противодействие актуальным угрозам информационной безопасности становятся первостепенной задачей как для государства, так и для всего общества. Таким образом, целью данной статьи является комплексный анализ актуальных вызовов и угроз информационной безопасности в российском обществе и правовом поле XXI в., а также осмысление перспектив развития механизмов их нейтрализации.

Так, понятие «информационная безопасность» традиционно определяется как состояние защищенности информационных потребностей личности, общества и государства от внешних и внутренних угроз. В XXI в. это определение расширяется, включая не только защиту данных и систем, но и обеспечение суверенитета в информационном пространстве, противодействие информационно-психологическому воздействию, поддержание стабильности критической информационной инфраструктуры (далее — КИИ).

В настоящее время можно рассуждать о том, что отчетливо сложились две модели международной информационной безопасности, а, именно: евразийская (Российская Федерация) и евроатлантическая. Основные задачи и направления развития информационной безопасности находят свое отражение в Указе Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» (далее — Стратегия) [6]. Характерной чертой закрепленных положений Стратегии является то обстоятельство, что они (положения и направления) направлены на разработку норм международного права, касающихся безопасности сетевого пространства и бесперебойного функционирования Сети интернет, определяя пределы юрисдикции права как национального, так и международных правовых механизмов в отношении субъектов глобальных информационных взаимоотношений [11, с 10]. Таким образом, можно заключить, что Стратегия в целом ориентирована на развитие информационной безопасности в масштабах международного права, обеспечиваемого сотрудничеством в области права с обязательным учетом общепризнанных принципов и норм международного права в условиях глобальной информационной интеграции и развития.

Следующей, не менее значимой проблемой в области обеспечения информационной безопасности можно назвать определение категории «информационная безопасность», поскольку само понятие «информационная безопасность» исследуется и рассматривается не только с правовой точки зрения. Так, рассмотрение информационной безопасности как подотрасли информационного права набирает все большие обороты в реалиях настоящего времени. В связи с чем указанные выше проблемы в области обеспечения информационной безопасности возможно решить, лишь скоординировав социальные, экономические, политические, организационные, информационные меры и усилия.

Так, основными направлениями обеспечения информационной безопасности в области обороны можно назвать: совершенствование системы обеспечения информационной безопасности самих сил обороны, включая средства информационного противостояния на возникающие киберугрозы; деятельность по сдерживанию и предотвращению военных конфликтов при помощи информационно-коммуникационных технологий, а также прогнозы, оценивание и обнаружение самих информационных угроз.

В качестве так называемых «общих» угроз при обеспечении информационной безопасности можно выделить:

1. Технологические угрозы. Данная категория охватывает «прямые» кибератаки и использование уязвимостей в цифровых системах [9, с. 8]. Использование уязвимостей в программном обеспечении и аппаратных решениях, уязвимости «нулевого дня», внедрение закладок на стадии производств и т. д.

2. Социально-психологические (информационно-психологические) угрозы. Эти угрозы направлены на манипуляцию сознанием, подрыв общественной стабильности и формирование негативных настроений, масштабное распространение дезинформации и фейковых новостей, целенаправленное информационно-психологическое воздействие.

3. Геополитические и стратегические угрозы. Связаны с использованием информационного пространства в рамках международного противоборства [10, с. 15]. Кибератаки на КИИ, цифровой суверенитет и зависимость от иностранных технологий, разведывательная деятельность в киберпространстве.

4. Экономические угрозы. Они направлены на получение финансовой выгоды или нанесение экономического ущерба (фишинг, атаки с использованием вредоносного программного обеспечения, мошенничество с использованием методов социальной инженерии, кража данных банковских карт).

Для эффективного противодействия актуальным вызовам и угрозам необходим комплексный и многовекторный подход: развитие технологического суверенитета; совершенствование правового регулирования, укрепление критической информационной инфраструктуры; развитие человеческого капитала; эффективное международное сотрудничество [8, с. 306]. Российская правовая система активно адаптируется к вызовам цифровой эпохи. Так, Основные положения по обеспечению информационной безопасности содержатся в Указе Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» (далее — Доктрина) [5]. Нельзя не упомянуть Конституцию Российской Федерации [1], Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3], Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [4], Федеральный закон от 26.07. 2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [2] и другие.

Несмотря на наличие серьезной правовой базы, существуют вызовы в ее эффективном применении, такие как: трансграничный характер угроз (многие кибератаки и информационные кампании инициируются за пределами России, что затрудняет применение национального законодательства и требует развития инструментов международного сотрудничества, что осложнено текущей геополитической ситуацией); стремительность технологического развития; проблемы правоприменения; баланс между безопасностью и свободами (обеспечение национальной информационной безопасности должно реализовываться без чрезмерного ограничения прав и свобод граждан).

Актуальные вызовы и угрозы информационной безопасности в российском обществе и праве XXI в. формируют сложный и динамичный ландшафт, требующий постоянного внимания и адаптивных решений. Стремительная цифровая трансформация, гибридные методы противоборства и усложнение киберпреступности ставят перед государством, обществом и правовой системой задачи, которые невозможно решить только техническими или только правовыми средствами. Лишь системный подход, сочетающий технологическое развитие, совершенствование законодательства, эффективную работу правоохранительных органов, повышение уровня осведомленности граждан и активное международное сотрудничество, позволит Российской Федерации эффективно противостоять угрозам, обеспечить национальную безопасность и реализовать свой потенциал в цифровом будущем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конституция Российской Федерации от 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования (01.07.2020). URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 25.08.2025).

2. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 25.08.2025).

3. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 25.08.2025).

4. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 25.08.2025).

5. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 05.12.2016 № 646. URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 25.08.2025).

6. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. : Указ Президента Российской Федерации от 09.05.2017 № 203 URL: https://www.garant.ru/products/ipo/prime/doc/71570570/ (дата обращения: 25.08.2025).

7. Агапов А. Б. Основы государственного управления в сфере информационных технологий : учебник. М. : Проспект, 2017. С. 304.

8. Бачило И. Л. Информационное право : учебник. 3-е изд., перераб. и доп. М. : Норма, 2017. С. 592.

9. Мамитов В. К. Правовое регулирование информационной безопасности: учебник для вузов. М. : Юрайт, 2022. С. 352.

10. Вайпан В. А. Правовое регулирование цифровой экономики в России: проблемы и перспективы // Право и экономика. 2021. № 2 (396). С. 5–12.

11. Демидов А. В., Мальцев А. И. Киберугрозы как элемент гибридных войн: правовые аспекты противодействия // Право и кибербезопасность. 2020. № 4. С. 12–18.