*УДК 004.056:341.47*

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГОСУДАРСТВА И МЕЖДУНАРОДНЫЕ ОБЯЗАТЕЛЬСТВА РОССИИ

© 2025 Е. Д. Сухарева[1], И. В. Евстафьева[2]

[1,2] Самарский университет государственного управления «Международный институт рынка», г. Самара, Россия

Информационные технологии играют ключевую роль в современном мире, оказывая значительное влияние на экономическое развитие, национальную безопасность и социальную стабильность каждой страны. Глобализация усиливает взаимозависимость государств, создавая новые риски и возможности. Международная среда характеризуется высоким уровнем неопределенности и угрозой возникновения конфликтов в виртуальном пространстве, что требует активного участия России в разработке и выполнении международных правил.

**Ключевые слова:** информационная безопасность, кибератаки, ментальная война, международные обязательства.

Информационная безопасность является одним из важнейших элементов современной политики любого государства. Ее значение значительно возросло с появлением Интернета и новых технологий связи, ставших частью повседневной жизни населения. Сегодня государство сталкивается с новыми угрозами – кибератаками, утечкой конфиденциальной информации, манипуляциями сознанием населения через вбросы недостоверной и откровенно ложной информации и другими формами цифрового воздействия.

Государства стремятся обеспечить свою безопасность, соблюдая национальные интересы и участвуя в международном диалоге, поскольку это позволяет защищать суверенитет, поддерживать внутреннюю стабильность, обеспечивать экономическую безопасность, противодействовать киберугрозам и эффективно взаимодействовать с другими странами в вопросах защиты информации.

Для того чтобы разобраться в теме, необходимо определить, что такое информационная безопасность.

Информация сама по себе имеет двойственную природу: с одной стороны, она представляет собой ресурс, способствующий развитию науки, культуры и экономики, с другой – может стать инструментом манипулирования общественным сознанием, угрозой политической стабильности и экономической конкурентоспособности.

Современное общество находится под постоянным воздействием различных источников информации, влияющих на формирование взглядов, убеждений и моделей поведения. Негативное воздействие может выражаться в распространении дезинформации, пропаганде экстремистских идей, формировании ложных стереотипов и предрассудков [1]. Для защиты от подобного влияния важно развивать критическое мышление, повышать медиаграмотность и укреплять механизмы контроля над информацией.

Важнейшая задача законодательства – установление правил обращения с информацией, защита прав граждан на доступ к информации, свободу выражения мнений и право на частную жизнь. Правовые меры включают разработку нормативных актов, регулирующих порядок сбора, хранения, обработки и распространения информации, защиту персональных данных и интеллектуальной собственности.

Важно отметить, что многие виды информации имеют стратегическое значение для государства и общества. К ним относятся государственная тайна, коммерческая тайна, персональные данные граждан и другие категории сведений, разглашение которых может нанести серьезный ущерб интересам государства, юридических лиц и физических лиц. Поэтому необходимы специальные меры защиты информации, такие как шифрование, ограничение дос-

тупа, контроль над использованием информационных технологий и системы мониторинга.

Итак, понимание сущности информации и ее роли в обеспечении безопасности государства требует комплексного подхода, включающего правовые, технические и организационные мероприятия, направленные на минимизацию рисков и повышение уровня информационной безопасности.

Таким образом, информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Информационная безопасность оказывает различное влияние на разные категории граждан, исходя из их особенностей и образа жизни. Рассмотрим ключевые группы и особенности их взаимодействия с вопросами информационной безопасности.

Граждане пожилого возраста зачастую испытывают трудности с пониманием современных технологий и мер защиты от киберпреступников. Из-за низкой компьютерной грамотности они легко становятся жертвами мошеннических схем, раскрывая свои личные данные и подвергаясь финансовым потерям. Таким образом, для пенсионеров чрезвычайно важен образовательный подход, направленный на повышение их осведомленности о базовых правилах информационной безопасности. Молодежь и подростки активно используют социальные сети и мобильные приложения, охотно делятся личной информацией и склонны доверять случайным контактам в Интернете. Эта группа особенно уязвима к социальным инженерным атакам, опасным сообществам и негативному влиянию через сеть. Родители и педагоги должны формировать у молодежи ответственное отношение к размещенной информации и научить их оценивать реальные риски общения в Интернете. Медийные лица и творческие работники подвержены нападениям через публикации неправдивой информации, которую используют недоброжелатели для разрушения репутации и нанесения вреда карьере. Такие граждане нуждаются в дополнительной поддержке и правовой охране от злоупотребления свободой слова и распространения заведомо ложных сведений.

Каждый гражданин обладает своими уникальными потребностями в отношении информационной безопасности, зависящими от его профессиональных обязанностей, жизненного опыта и характера деятельности. Осознанное поведение и знание элементарных принципов защиты способствуют уменьшению числа инцидентов и повышают общий уровень защищенности всей страны.

Государства сталкиваются с множеством угроз в цифровой среде, которые существенно влияют на их безопасность и развитие. Рассмотрим основные группы таких угроз.

Киберугрозы и кибератаки стали одним из наиболее опасных факторов, угрожающих национальной безопасности. Их цели разнообразны: шпионаж, саботаж, вымогательство, идеологическое влияние, диверсии, дестабилизация политической ситуации, экономический ущерб и даже нанесение физического урона объектам критически важной инфраструктуры.

Типичные формы проявления кибератак многообразны. Например, DDoS-атаки способны парализовать работу онлайн-сервисов, учреждений государственного управления, платежных систем и СМИ. Фишинг-мошенничества направлены на хищение персональной информации граждан и организаций, используются для компрометации аккаунтов, банковских карт и прочих чувствительных данных. Хакерские взломы позволяют получать доступ к закрытым ресурсам и базам данных, открывают возможности для промышленного и политического шпионажа.

Кроме того, широкое распространение получили вирусные инфекции типа троянов, шпионского ПО используемых для заражения компьютеров и мобильных устройств, последующего извлечения ценной информации либо формирования распределенных сетей для дальнейших атак. Отдельно выделяются целевые атаки APT (Advanced Persistent Threat), осуществляемые профессиональными группами высо-

коквалифицированных специалистов, преследующих долгосрочные политические и военные цели [2].

Сбор и утечка персональных данных являются немаловажными проблемами, стоящими перед государством в рамках обеспечения информационной безопасности. Персональные данные представляют особый интерес для злоумышленников ввиду содержащейся в них конфиденциальной информации, которая может использоваться для шантажа, мошенничества, шпионажа и иных противоправных деяний.

Современные цифровые технологии значительно упростили процесс сбора персональных данных, создав благоприятные условия для массовых нарушений конфиденциальности. Повсеместное использование Интернета, социальных сетей, облачных сервисов и приложений открывает широкие возможности для отслеживания перемещения граждан, определения их предпочтений, контактов и иной частной информации. Часто сбор осуществляется легально, однако нередко встречаются случаи нелегального аккумулирования данных, нарушающие права граждан на неприкосновенность частной жизни. Незаконное использование личных данных гражданами и компаниями для коммерческих или политических целей. Чаще всего такие инциденты происходят по следующим причинам: взлом компьютерных систем, потеря устройств, ошибка персонала, несовершенство технических средств защиты. Наиболее известные случаи утечек данных касаются крупных банков, социальных сетей и правительственных ведомств. Например, широко известны инциденты с Facebook, Equifax и Yahoo!, приведшие к компрометации миллионов учетных записей.

Ментальное воздействие, или ментальная война, представляет собой форму информационного давления, нацеленного на изменение мировоззрения, психологического состояния и поведенческих установок противника. В отличие от классических военных конфликтов, где доминируют традиционные методы боевых действий, ментальные операции проводятся преимущественно скрытыми способами и действуют на уровне сознания и подсознания. Основными инструментами такого воздействия служат средства массовой информации, социальные сети, киноиндустрия, литература и культурные проекты.

Россия сталкивается с множеством вызовов в области ментальной войны, вызванных усилением внешнего информационного давления. Отечественная концепция ментальной обороны строится на принципах укрепления идентичности, сохранения культурного наследия и воспитания патриотизма. Эти принципы реализуются через систему образовательных программ, просветительских кампаний и мероприятий, направленных на сохранение исторической памяти и традиций. Особое внимание уделяется созданию устойчивых медиаресурсов, формирующих позитивный образ страны и препятствующих внедрению чуждых ценностных ориентиров [3].

Эффективность ментальной обороны зависит от способности государства оперативно реагировать на внешние угрозы, быстро адаптироваться к изменениям среды и поддерживать высокий уровень доверия населения к официальным источникам информации. Российские специалисты предлагают ряд инициатив, направленных на изучение природы ментального воздействия, выработку рекомендаций по укреплению иммунитета общества к враждебным пропагандистским кампаниям и построению комплексной системы защиты национальной ментальности.

Россия имеет развитое законодательство, направленное на регулирование вопросов информационной безопасности. Среди наиболее значимых правовых актов выделяются:

- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»; этот документ регулирует основы обращения с информацией в электронном виде, устанавливает правила сбора, обработки и распространения сведений [4];
- Указ Президента РФ от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации», который определяет главные приоритеты госу-

дарства в условиях возникновения кризисных ситуаций, включая угрозу нарушения IT-безопасности [5];

- Доктрина информационной безопасности Российской Федерации – документ, утверждаемый Президентом РФ, он формулирует принципы и методы обеспечения защиты информации, содержащие государственную тайну и персональные данные граждан.

Эти законы обеспечивают возможность контролировать доступ к персональным данным, защищать государственные секреты и ограничивать использование иностранного программного обеспечения в стратегических отраслях.

Перейдем к международным обязательствам. Россия, обладая развитым информационным пространством и значительным влиянием в международной политике, активно участвует в формировании глобальных стандартов информационной безопасности и принимает участие в различных международных соглашениях и инициативах. Одним из примеров являются соглашения в рамках ШОС и СНГ. Государства, входящие в Шанхайскую организацию сотрудничества (ШОС) и Содружество Независимых Государств (СНГ), подписали двусторонние и многосторонние соглашения о взаимодействии в области IT-безопасности. Эти документы предусматривают регулярные консультации, совместное обучение специалистов, обмен информацией о потенциальных угрозах и разработку общих механизмов реагирования на атаки. Такими соглашениями являются:

- Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности (2009 г.);
- Меморандум о взаимопонимании между странами ШОС по вопросам обеспечения региональной безопасности в информационной сфере (2016 г.).

Эти договоренности направлены на снижение риска кибертерроризма, защиту государственной тайны и стратегических объектов от несанкционированного вмешательства извне.

Международные обязательства России в рамках ОДКБ по информационной безопасности. Вступив в Организацию Договора о коллективной безопасности (ОДКБ), Российская Федерация взяла на себя целый ряд значимых обязанностей, среди которых особое место занимают именно обещания в области IT-безопасности. Согласно подписанному соглашению, Россия обязуется своевременно передавать другим членам ОДКБ достоверную информацию о возникновении потенциальных угроз информационной безопасности, обнаруживаемых уязвимостях в системах и мерах, принимаемых для их устранения. Такое обязательство обеспечивает быструю реакцию на потенциальные инциденты и снижает вероятность нанесения ущерба участникам организации. Также все участники обязана оказывать содействие другим странам – участницам ОДКБ в обучении сотрудников специализированных служб, участвующих в обеспечении IT-безопасности. Это предполагает организацию курсов, семинаров и тренингов, передачу технологий и методики подготовки квалифицированных специалистов [6].

Несмотря на уже существующие соглашения, Россия регулярно предлагает международным партнерам обсудить возможность подписания единого международного акта, определяющего рамки допустимого поведения в цифровом пространстве. Цель такой инициативы – минимизация конфликтов, связанных с несанкционированным доступом к ресурсам и инфраструктурам, защита конфиденциальной информации и предотвращение нарушения суверенитета государств.

Таким образом, можно говорить о том, что современное российское законодательство и международная политика формируют прочный фундамент для обеспечения информационной безопасности государства. Правовая система Российской Федерации устанавливает требования к информационной безопасности, контроль над использованием информационных технологий и защиту конфиденциальных сведений. Россия активно сотрудничает в рамках ШОС, СНГ, ОДКБ, развивая механизмы совместного реагирования на современные

цифровые угрозы. Вместе с тем новые формы угроз, такие как ментальные войны, кибератаки и утечки данных, продолжают представлять серьезную опасность для государства и общества. Решение этих проблем требует комплексного подхода, сочетающего правовые, технологические и образовательные меры. Формирование грамотной информационной культуры граждан, развитие отечественных IT-решений и постоянное обновление правовых норм позволят России успешно адаптироваться к изменениям и сохранить лидерство в вопросах обеспечения информационной безопасности.

СПИСОК ИСТОЧНИКОВ

1. Минаев Э. Е. Формирование концепции государственной информационной безопасности России // Вестник Академии военных наук. 2020. № 4. С. 21-27.
2. Снытников А. А. Лицензирование и сертификация в области защиты информации. М.: Гелиос АРВ, 2003. 192 с.
3. Ильницкий А. М. Ментальная война России // Военная мысль. 2021. № 12. С. 19-26.
4. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»// СПС «КонсультантПлюс». URL: https://www.consultant.ru/.
5. Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/.
6. Воробьев Н. Н. Международные обязательства России в области информационной безопасности // Государство и право. 2022. № 3. С. 34-41.

## INFORMATION SECURITY OF THE STATE AND RUSSIA INTERNATIONAL OBLIGATIONS

© 2025 Ekaterina D. Sukhareva[1], Irina V. Evstafieva[2]

[1,2]Samara University of Public Administration
“International Market Institute”, Samara, Russia

Information technologies play a key role in the modern world, having a significant impact on the economic development, national security and social stability of each country. Globalization increases the interdependence of States, creating new risks and opportunities. The international environment is characterized by a high level of uncertainty and the threat of conflict in the virtual space, which requires Russian active participation in the development and implementation of international rules.

**Keywords:** information security, cyber attacks, mental warfare, international obligations.