

Основные угрозы информационной безопасности

Ш. Г. Утарбеков

Челябинский государственный университет, Челябинск, Россия

Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы. Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

Ключевые слова: *информация, информационная безопасность, защита права.*

Практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз¹.

Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Российские средства массовой информации зачас-

тую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности.

Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными

¹ Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // КонсультантПлюс (дата обращения 22.07.2021).

государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности.

Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обуславливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции, зачастую не имеют комплексной основы.

Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.

Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети Интернет, не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими.

Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности. Кроме того, в нашей стране был задействован целый комплекс мероприятий, предусмотренных государственной программой Российской Федерации «Информационное общество (2011–2020 годы)», утвержденной Постановлением Правительства РФ от 15.04.2014 № 313, программой «Цифровая экономика Российской Федерации», утвержденной распоряжением Правительства РФ от 28.07.2017 № 1632-р, и др.

Представляется очевидным, что бурное развитие цифровых технологий, отмечающееся в последние годы, имеет своим следствием трансформацию самых разнообразных слагаемых общественной жизни и не может не сказаться на состоянии правового регулирования и на правоприменительной практике. Это воздействие технического прогресса на правовую среду правоведа на теоретическом уровне связывают в первую очередь со сферами гражданского права, информационного права, финансового права и других отраслей некриминального блока. Именно их предметами охватывается наиболее обширный перечень общественных отношений, имеющих сво-

им элементом оцифрованную информацию. Тем не менее такие сферы правового регулирования, которые традиционно в наименьшей степени подвержены какому-либо влиянию извне, относятся к наиболее консервативному сектору права, в частности правовое регулирование уголовно-юрисдикционной деятельности, и не могут не испытывать

на себе соответствующего трансформирующего эффекта цифровизации.

В связи с этим представляется необходимым с научных позиций комплексно рассмотреть вопросы, связанные с цифровизацией уголовно-юрисдикционной деятельности.

Дата поступления: 20.12.2021

Дата принятия к опубликованию: 22.12.2021

Сведения об авторе

Утарбеков Шамиль Галимович — кандидат юридических наук, доцент кафедры конституционного и муниципального права Института права Челябинского государственного университета, Челябинск, Россия. law@csu.ru

Библиографическое описание: Утарбеков, Ш. Г. Основные угрозы информационной безопасности / Ш. Г. Утарбеков // Вестник Челябинского государственного университета. Серия: Право. — 2021. — Т. 6, вып. 4. — С. 49–51. — DOI: 10.47475/2618-8236-2021-16409.

Bulletin of Chelyabinsk State University. Series: Law. 2021. Vol. 6, iss. 3. Pp. 49–51.

Main Threats to Information Security

Sh. G. Utarbekov

Chelyabinsk State University, Chelyabinsk, Russia. law@csu.ru

The expansion of the fields of application of information technologies, being a factor in the development of the economy and improvement of the functioning of public and state institutions, at the same time generates new information threats. The possibilities of cross-border circulation of information are increasingly being used to achieve geopolitical, military-political, as well as terrorist, extremist, criminal and other illegal goals at the expense of international security and strategic stability.

Keywords: *information, information security, protection of law.*