Научная статья
УДК 342

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Беляева Ольга Васильевна
Орловский юридический институт МВД России имени В.В. Лукьянова, Орел, Россия

Julia18flash@yandex.ru

Аннотация. С опорой на научные и прикладные исследования в статье рассматривается современная практика внедрения информационных технологий без обязательной увязки с обеспечением информационной безопасности, что существенно повышает вероятность проявления прежних и появления новых информационных угроз, среди которых особенно значимы такие проблемы, как нарастающее информационное/цифровое неравенство, возможности манипуляции общественным сознанием, киберболезни (компьютерная зависимость и др.), компьютерная преступность (киберпреступность), информационные войны и др. Подчёркивается, что исследования информационной безопасности личности в России являются ключевым элементом обеспечения безопасности, стабильности и развития общества в условиях современных информационных технологий.

Ключевые слова: глобализация, информационные технологии, искусственный интеллект, угрозы информационной безопасности.

Для цитирования: Беляева О. В. Информационная безопасность личности в глобальном информационном пространстве // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2025. № 2(103). С. 36–43.

PERSONAL INFORMATION SECURITY IN THE GLOBAL INFORMATION SPACE

Olga V. Belyaeva
Lukyanov Orel Law Institute of the Ministry of the Interior of Russia, Orel, Russia

Julia18flash@yandex.ru

Annotation. Based on scientific and applied research, the article examines the modern practice of introducing information technologies without necessarily linking them to information security, which significantly increases the likelihood of former and new information threats, among which such problems as increasing information/digital inequality, the possibility of manipulating public consciousness, cyber-diseases (computer addiction, etc.) are particularly significant.), computer crime (cybercrime), information warfare, etc. The article emphasizes that research on personal information security in Russia is a key element in ensuring the security, stability and development of society in the context of modern information technology.

Keywords: globalization, information technology, artificial intelligence, threats to information security.

For citation: Belyaeva O. V. Information security of the individual in the global information space // Scientific Bulletin of the Orel Law Institute of the Ministry of Internal Affairs of Russia named after V.V. Lukyanov. 2025. № 2(103). P. 36–43.

Активное развитие информационно-коммуникационных технологий и цифровая трансформация экономических процессов привели не только к появлению новых видов цифровых услуг, возникновению белых, серых, чёрных (теневых) экономических рынков, структурной трансформации секторов экономики, но также и к новой системе социально-экономических отношений, формирующейся в глобальном информационно-экономическом пространстве.

Возможности динамично развивающихся информационных технологий и средств массовых коммуникаций, которые могут управлять информационными потоками с помощью информационных фильтров, позволяют злоумышленникам, манипулируя социальными проблемами и потребностями населения, с помощью методов социальной инженерии и информационно-психологического воздействия вовлекать людей в сомнительные экономические и мошеннические проекты, в социально опасную деятельность; распространять идеи экстремистского характера; развязывать межличностные, социальные и межнациональные конфликты; формировать низкопробную массовую культуру; продвигать интересы определённых групп и сообществ; навязывать собственные стандарты поведения, модели потребления и восприятия информации, оказывая деструктивное воздействие в масштабах регионального, национального и глобального информационного пространства. Актуальность исследования данного вопроса обусловлена тем, что проблема противоправного деструктивного информационно-психологического воздействия на личность, общество и государство стала одной из современных глобальных проблем мирового сообщества.

Вместе с тем авторы ряда работ обращают внимание на то, что с правовой точки зрения, дефиниция «вредоносное информационное воздействие», осуществляемое в интересах определённых политических и социальных сил и оказывающее негативное деформирующее влияние на личность, общество и информационно-психологическую среду государства, не имеет официального закрепления, а закрепление новых составов преступлений в сфере информационных технологий должно соответствовать тенденциям развития современной преступности и учитывать анализ квалификационных признаков преступлений по каждой статье Уголовного кодекса. Выявление реальных информационно-психологических, экономических и правовых угроз, существующих в современном информационном пространстве, часто затруднено в связи с отсутствием непосредственного контакта между объектом посягательств и злоумышленниками, ощущающими недосягаемость и безнаказанность. Категория «информационная безопасность личности» также требует закрепления в действующем законодательстве, что разрешит ряд проблем, связанных с терминологией, содержанием. По мнению Кузьменкова Т. Н., юридическую проработку проблем информационной безопасности личности целесообразно вести отдельно по техническим и содержательным (смысловым) компонентам [1, с. 72].

Бражник Т. А. отмечает, что, несмотря на то что информационная безопасность личности является важнейшим элементом национальной информационной безопасности, анализ специальных нормативных документов показывает, что на уровне двустороннего международно-правового сотрудничества, в ряде определений, связанных с трактовками информационной безопасности государства в целом и информационной безопасности личности, существуют определённые противоречия. В частности, определение информационной безопасности личности как состояния защищённости от внешних

и внутренних угроз неоднородно и применимо преимущественно для технической сферы [2, с. 188].

Представляется возможным согласиться с Алексеевой Л. А., подчёркивающей, что «формируется новая, реальная многополярность, требующая от государств выстраивания системы постоянного мониторинга предполагаемых и возможных в сегодняшних условиях угроз» [3, с. 40]. И действительно, проблемы формирования системы международной информационной безопасности, по мнению целого ряда авторов [4, с. 138], необходимо рассматривать в контексте возникновения новых угроз, трансформации права и глобальной проблемы «инфодемии». Целенаправленное информационно-психологическое воздействие, осуществляемое с помощью информационно-телекоммуникационных технологий, может быть направлено и на представителей различных государственных структур, на сотрудников правоохранительной сферы, а также на широкие круги населения с целью вовлечения их в противоправную антиобщественную и антигосударственную деятельность. В оказании такого воздействия могут быть заинтересованы представители преступных сообществ и отдельных криминальных элементов, коммерческих и некоммерческих организаций, несистемных оппозиционных политических объединений. К угрозам и противоправным действиям, направленным на подрыв системы информационной безопасности государства, следует относить действия, связанные в том числе с незаконным оборотом наркотических средств и цифровых валют; с социальной инженерией; с сексуальной эксплуатацией несовершеннолетних; с распространением и использованием информации, приносящей вред общественной нравственности и здоровью населения; с распространением деструктивных и экстремистских материалов. Нелегальные материалы и информация могут распространяться, например с помощью СМС рассылок, различных рекламных сайтов и мессенджеров.

Сотрудники государственных служб могут подвергаться информационно-психологическим атакам через традиционные средства коммуникаций и передачи информационных сообщений, к которым, в частности, могут быть отнесены средства телефонной связи и печатная продукция, включающая рекламные листки и объявления. Информационно-психологическому воздействию могут подвергаться и сотрудники силовых структур, которые в личной жизни в большей или меньшей степени, но обращаются к инструментам социальных сетей, обеспечивающих продвижение цифрового контента. К таким инструментам, через которые может быть оказано информационно-психологическое воздействие, следует отнести, например сайты для обмена фотографиями и видеоконтентом, микроблоги, автоматически генерируемые новостные RSS-каналы (*Rich Site Summary*) [5, с. 34].

Цели такого воздействия могут быть связаны с попытками криминальных элементов использовать служебное положение представителей силовых структур, мотивировав их к уклонению от корректного выполнения должностных обязанностей и создав препятствия для решения поставленных перед ними оперативно-служебных задач. Деструктивное информационно-психологическое воздействие на сотрудников правоохранительной сферы может быть ориентировано на создание у сотрудников состояния тревоги за своё будущее и искажённого ощущения реальных и вымышленных угроз, размывание чувства и гордости за свою страну. Деструктивное воздействие может быть направлено не только на изменение сознания, самовосприятия и психологического состояния отдельных сотрудников, но и на деформацию социальных отношений в коллективе путём создания состояния групповой подавленности или конфликтности. К числу важнейших элементов системы защиты как сотрудников государственных служб, так и пользователей социальных сетей от угроз

и деструктивного воздействия глобального информационного пространства следует отнести психологическую устойчивость участников социальных коммуникаций.

Экономические права граждан могут нарушаться со стороны злоумышленников с преступными корыстными мотивами. К типичным экономическим угрозам в интернете следует отнести, например действия хакеров, направленные на кражи криптоценностей и средств, принадлежащих гражданам и хранящимся на банковских депозитах. Получение доступа к личным данным владельцев банковских вкладов может осуществляться как, например, с помощью различных мошеннических приёмов, связанных с социальной инженерией и информационно-психологическим воздействием на потенциальных жертв, так и с помощью создания поддельных сайтов и аккаунтов. В частности, такие угрозы представляют злоумышленники, эксплуатирующие болезненные состояния потенциальных жертв и стимулирующие их к игровым зависимостям (интернет-аддикции). Интернет-аддикция представляет собой форму изменённого психического состояния и поведения, связанную с пагубными привычками, компьютерными и игровыми зависимостями и уходом в виртуальную реальность. Органы государственной власти и институты гражданского общества постоянно совершенствуют правовые рычаги для защиты детей и молодого поколения от тлетворного негативного информационно-психологического влияния глобального информационного пространства.

Однако, по мнению Чимарова С. Ю., Чимарова Н. С. [6, с. 71], для решения проблем интернет-аддикции необходима совместная работа многих специалистов, так как, несмотря на разрозненные усилия психологов, юристов, медиков и педагогов, число интернет-зависимых людей, часто не осознающих этой зависимости, не только не уменьшается, а постоянно увеличивается. К деструктивным молодёжным субкультурам, представители которых демонстрируют признаки психических заболеваний и представляют угрозы для личности, общества и государства, можно отнести суицидальные субкультуры («группы смерти»), депрессивные, радикальные, агрессивные и девиантные сообщества; а также группы, поддерживающие вооружённые нападения злоумышленников на учащихся внутри учебных заведений (скулшутинг).

Жертвами преступников, профессионально владеющих приёмами информационно-психологического воздействия, могут легко стать дети и подростки, не имеющие достаточного жизненного опыта и навыков критического анализа информации. В работе Ратникова И. Г. отмечено [7, с. 322], что информационно-психологическими последствиями бесконтрольного доступа детей к интернету могут стать: знакомство детей с потенциально опасными людьми; нарушение нормального развития ребёнка; неправильное формирование нравственных ценностей и киберзависимость.

Жертвами злоумышленников могут также стать взрослые люди, для психологического портрета которых характерны в первую очередь следующие черты: инфантильность, внушаемость, восприимчивость к воздействию на когнитивно-эмоциональную сферу; отсутствие навыков и способностей к анализу потенциальных рисков; отсутствие склонности к критическому восприятию информации; безответственные решения и стремление к достижению «лёгких результатов», эмоциональный тип мышления и «клиповая психология» [8, с. 44].

В свою очередь, в ряде случаев не только жертвы, попавшие в психологическую зависимость, но и их друзья и родственники могут быть вовлечены в преступные схемы, невольно став исполнителями кем-либо запрограммированных действий. Не только сами действия, нарушающие законы государства и предполагающие уголовное преследование, но и обсуждение намерений, а также и подготовка к совершению преступных действий, могут осуществляться с помощью различных психологических приёмов, использующих различные информационно-коммуникационные технологии. Как правило, информационно-психологическое

воздействие ориентировано на изменение информационного статуса или личностных характеристик объекта воздействия и осуществляется с помощью определённым образом оформленной и декларируемой информации.

В качестве целенаправленных методов воздействия обычно используются методы внушения, убеждения, заражения и стимулирования к подражанию. Инструментальной основой психологического давления и доставки угроз и оскорблений до жертвы могут выступать СМС рассылки, звонки с мобильных телефонов, мгновенные сообщения и электронные письма. В связи с тем что оскорбления, насмешки и провокации могут поступать с разных адресов электронной почты или номеров телефонов, защита от злоумышленников с помощью «чёрных и белых списков» не всегда является достаточно эффективной. В качестве инструментальных средств для осуществления «криминальной деятельности» могут выступать анонимные почтовые серверы; зеркала Фейсбука, запрещённого в некоторых странах; различные сайты, на которых реализованы форумы об оружии; анонимные торговые площадки для наркобизнеса и для торговли криптовалютой. В манипулятивный набор применяемых психотехнологий с целями психологического воздействия могут входить различные приёмы и способы подачи информации с учётом социального контекста, момента и выгодного физического фона для подачи информации. К таким приёмам следует отнести, например: ложь, смещение понятий, утаивание деталей и важных аспектов; искажение; компоновку тем; подтасовку фактов; манипулирование предрассудками; создание потока бессмысленной информации [3, с. 41].

Современные информационно-коммуникационные инструменты позволяют злоумышленникам реализовать психотехнику так называемого «кибербуллинга», оказывая круглосуточное давление на участников информационных коммуникаций, в частности на сотрудников правоохранительных органов, и распространяя фейковую или компрометирующую информацию для практически неограниченной аудитории. В ряде случаев инструментом воздействия на потенциальных жертв являются угрозы информационно-психологического воздействия и психологические атаки, использующие методы психологического травмирования пользователя с помощью контента брутального содержания. В качестве инструментов информационно-психологического воздействия на широкий круг лиц, например в сфере общественной деятельности, также может применяться технология так называемого «краудсорсинга», которая позволяет с помощью информационно-технических средств вовлечь большое количество участников в процесс достижения поставленных целей на добровольных началах или за незначительное вознаграждение.

Сложность решения многих проблем правовой, экономической и информационно-психологической безопасности личности и государства обусловлена целым рядом обстоятельств, к которым относится в том числе то, что глобальное информационное пространство представляет собой открытую систему с отсутствием централизованного управления, а неоднозначность подходов мирового сообщества к оценке информационных угроз, проблемных контентов и признаков деструктивной информации создаёт барьеры для установления единых стандартов.

На международном уровне отсутствует единство мнений относительно терминологии и наполнения понятий «информационная безопасность» и «информационная безопасность личности». Регулирование информационных потоков в глобальном пространстве интернета осуществляется отдельными государствами и частными компаниями на основе действующих и изменяющихся правовых и организационных мер, имеющих как разрешительный, так и запретительный характер. Отсутствие централизованного управления глобальным интернет-пространством обусловлено целым рядом правовых и имущественных обстоятельств,

в соответствии с которыми многие компоненты интернет-инфраструктуры принадлежат крупнейшим государственным или частным телекоммуникационными компаниям. Владельцы межконтинентальных оптоволоконных линий и телефонных сетей, спутников связи, маршрутизаторов, центров обработки данных по своему усмотрению могут сдавать в аренду сетевые ресурсы не только крупным провайдерам, но и мелким операторам, работающим с конечными потребителями, которые, в свою очередь, с помощью различных экономических рычагов, касающихся размеров оплаты за предоставляемое в аренду оборудование, трафик и различные сервисы, могут ограничивать коммуникационные возможности граждан.

Возможности скрытых сетей по организации бесконтрольной и анонимной передачи информации являются своего рода гарантией безопасности и безнаказанности для различного рода злоумышленников и правонарушителей, позволяя им эффективно реализовывать преступные замыслы, что может способствовать формированию ощущения вседозволенности и безнаказанности при совершении противоправных действий у всех пользователей, работающих в сети «*DarkNet*».

По мнению Рожкова А. А. и Аникеевой Н. В. [9, с. 32], для обеспечения информационной безопасности необходимо создание единого международного правового пространства. Вместе с тем несмотря на то что в настоящее время в РФ происходит постепенное формирование информационного законодательства, законодательные инициативы носят порой разрозненный характер, а вопросы, связанные с концептуальной основой обеспечения национального информационного суверенитета, как и с обеспечением устойчивости, стабильности, защищённости, непрерывности и целостности функционирования национального сегмента сети Интернет, нуждаются в дальнейшей доработке.

По мнению Сергун П. П. и Герасимова Ю. С. [10, с. 114], к важнейшим принципам, которые должны быть положены в основу создания системы информационной безопасности личности, следует отнести принцип международного сотрудничества в сфере информационной безопасности, реализация которого предполагает международный обмен опытом и оценку эффективности мер, принятых для решения конкретных проблем. Для создания эффективных механизмов международного регулирования в условиях больших вызовов в глобальном информационном обществе необходима разработка современных моделей и новых подходов для прогнозирования перспектив развития и трансформации международных норм информационной безопасности. В том случае если мировое сообщество придёт к пониманию необходимости формирования безопасного глобального виртуального пространства с помощью международных структур централизованного управления, потребуется разработка единой нормативно-правовой базы; формирование органов управления международного уровня; создание структур для предупреждения и пресечения противоправных действий, для выявления преступного контента, для расследования инцидентов и преступных сделок в глобальной сети [11, с. 346].

Таким образом, по результатам проведённого исследования и на основании указанных примеров можно сделать вывод, что проблемы, связанные с информационной безопасностью личности и государства, актуальны, имеют комплексный характер и должны решаться системными методами. Терминологическая база категории информационной безопасности требует постоянного правового сопровождения и актуализации. Целесообразной следует считать разработку моделей информационных угроз, психологических портретов и мотивов злоумышленников, осуществляющих преступные действия с помощью современных информационных технологий. Для решения проблем информационной безопасности в масштабах глобального информационного пространства необходимы усилия всего мирового сообщества.

1. Кузьменкова Т. Н. Проблемные аспекты правового сопровождения информационной безопасности личности // Проблемы устойчивого развития регионов Республики Беларусь и сопредельных стран : сборник научных статей XI Международной научно-практической интернет-конференции / под редакцией Н. В. Маковской. Могилев, 2022. С. 71–74.
2. Бражник Т. А. Отдельные аспекты правового регулирования информационной безопасности личности // Вестник Воронежского государственного университета. Серия: Право. 2019. № 3(38). С. 182–189.
3. Алексеева Л. А., Майорова С.А. К вопросу о государственном суверенитете в условиях глобализации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 3(59). С. 39–44.
4. Полякова Т. А., Шинкарецкая Г. Г. Проблемы формирования системы международной информационной безопасности в условиях трансформации права и новых вызовов и угроз // Право и государство: теория и практика. 2020. № 10 (190). С. 138–142.
5. Мушта А. А. Проблемные аспекты защищенности органов безопасности и правопорядка от деструктивного информационного воздействия // Деятельность правоохранительных органов на современном этапе: наука, образование, практика: сборник статей по итогам VI Международного научно-практического семинара. Минск, 2021. С. 33–35.
6. Чимаров С. Ю., Чимаров Н. С. Правовое регулирование вопросов сетевой безопасности сотрудников органов внутренних дел в контексте ведомственных нормативных правовых актов // Проблемы современного законодательства России и зарубежных стран. Материалы X Международной научно-практической конференции / отв. редакторы А. М. Бычкова, Н. В. Кешикова. Иркутск, 2021. С. 70–74.
7. Ратникова И. Г. О необходимости профилактики интернет-аддикции как вида психологической зависимости и о некоторых правовых аспектах в сфере информационной безопасности детей // Дни науки. Сборник трудов международной научно-практической конференции. В 2-х ч. / под редакцией В. И. Бакайтис, 2018. С. 319–324.
8. Смирнов А. А. Роль и функции МВД России в системе обеспечения информационно-психологической безопасности // Научный портал МВД России. 2022. № 2(58). С. 41–49.
9. Рожков А. А., Аникеева Н.В. Психолого-педагогические условия противодействия информационно-психологическим угрозам в служебной деятельности // Морально-психологическое обеспечение деятельности органов внутренних дел: современные подходы и перспективы развития. Материалы всероссийской научно-практической конференции. СПб.: Санкт-Петербургский университет МВД России, 2022. С. 30–35.
10. Сергун П. П., Герасимов Ю. С. Информационная безопасность в Российской федерации: отдельные аспекты правового регулирования. Вестник Российской правовой академии. 2020. № 2. С. 112–117.
11. Смольяков А. А. К вопросу о защите прав и свобод человека и гражданина в контексте информационной безопасности личности // Закон. Право. Государство. 2022. № 2(34). С. 344–350.

1. Kuz`menkova T. N. Problemny`e aspekty` pravovogo soprovozhdeniya informacionnoj bezopasnosti lichnosti // Problemy` ustojchivogo razvitiya regionov Respubliki Belarus` i sopredel`ny`x stran : sbornik nauchny`x statej XI Mezhdunarodnoj nauchno-prakticheskoj internet-konferencii / pod redakciej N. V. Makovskoj. Mogilev, 2022. S. 71–74.
2. Brazhnik T. A. Otdel`ny`e aspekty` pravovogo regulirovaniya informacionnoj bezopasnosti lichnosti // Vestnik Voronezhskogo gosudarstvennogo universiteta. Se-riya: Pravo. 2019. № 3(38). S. 182–189.

3. Alekseeva L. A., Majorova S.A. K voprosu o gosudarstvennom suverenitete v usloviyax globalizacii // Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoj akademii MVD Rossii. 2022. № 3 (59). S. 39–44.
4. Polyakova T. A., Shinkareczkaya G. G. Problemy` formirovaniya sistemy` mezhdunarodnoj informacionnoj bezopasnosti v usloviyax transformacii prava i novy`x vy`zovov i ugroz // Pravo i gosudarstvo: teoriya i praktika. 2020. № 10 (190). S. 138–142.
5. Mushta A. A. Problemny`e aspekty` zashhishhennosti organov bezopasnosti i pravoporyadka ot destruktivnogo informacionnogo vozdejstviya // Deyatel`nost` pravooxranitel`ny`x organov na sovremennom e`tape: nauka, obrazovanie, praktika : sbornik statej po itogam VI Mezhdunarodnogo nauchno-prakticheskogo seminara. Minsk, 2021. S. 33–35.
6. Chimarov S. Yu., Chimarov N. S. Pravovoe regulirovanie voprosov setevoj bezopasnosti sotrudnikov organov vnutrennix del v kontekste vedomstvenny`x normativ-ny`x pravovy`x aktov // Problemy` sovremennogo zakonodatel`stva Rossii i zarubezhny`x stran. Materialy` X Mezhdunarodnoj nauchno-prakticheskoj konferencii / otv. redaktory` A. M. By`chkova, N. V. Keshikova. Irkutsk, 2021. S. 70–74.
7. Ratnikova I. G. O neobxodimosti profilaktiki internet-addikcii kak vida psixologicheskoj zavisimosti i o nekotory`x pravovy`x aspektax v sfere informaci-onnoj bezopasnosti detej // Dni nauki. Sbornik trudov mezhdunarodnoj nauchno-prakticheskoj konferencii. V 2-x ch. / pod redakciej V. I. Bakajtis, 2018. S. 319–324.
8. Smirnov A. A. Rol` i funkcii MVD Rossii v sisteme obespecheniya informaci-onno-psixologicheskoj bezopasnosti // Nauchny`j portal MVD Rossii. 2022. № 2 (58).S. 41–49.
9. Rozhkov A. A., Anikeeva N.V. Psixologo-pedagogicheskie usloviya protivodej-stviya informacionno-psixologicheskim ugrozam v sluzhebnoj deyatel`nosti // Moral`-no-psixologicheskoe obespechenie deyatel`nosti organov vnutrennix del: sovremenny`e podxody` i perspektivy` razvitiya. materialy` vserossijskoj nauchno-prakticheskoj konferencii. SPb.: Sankt-Peterburgskij universitet MVD Rossii, 2022. S. 30–35.
10. Sergun P. P., Gerasimov Yu. S. Informacionnaya bezopasnost` v Rossijskoj fe-deracii: otdel`ny`e aspekty` pravovogo regulirovaniya. Vestnik Rossijskoj pravovoj akademii. 2020. № 2. S. 112–117.
11. Smol`yakov A. A. K voprosu o zashhite prav i svobod cheloveka i grazhdanina v kontekste informacionnoj bezopasnosti lichnosti // Zakon. Pravo. Gosudarstvo. 2022. № 2(34). S. 344–350.

Информация об авторе

Ольга Васильевна Беляева. Доцент кафедры государственно-правовых дисциплин, кандидат юридических наук, доцент.
Орловский юридический институт МВД России имени В.В. Лукьянова.
302027, Россия, г. Орел, ул. Игнатова, 2.

Information about the author

Olga V. Belyaeva. Associate Professor of the Department of State and Legal Disciplines. Candidate of Law, Associate Professor.
Lukyanov Orel Law Institute of the Ministry of the Interior of Russia.
302027, Russia, Orel, Ignatov Str., 2.

Статья поступила в редакцию 25.03.2025; одобрена после рецензирования 01.04.2025; принята к публикации 17.06.2025.
The article was received in the editorial office on 25.03.2025; approved after review on 01.04.2025; accepted for publication on 17.06.2025.