Проект

Концепция информационно-психологической безопасности в Российской Федерации[1]

I. Общие положения

1. Настоящая Концепция представляет собой систему взглядов на обеспечение информационно-психологической безопасности как части информационной и национальной безопасности Российской Федерации.

2. Настоящей Концепцией определяются основные угрозы информационно-психологической безопасности в Российской Федерации, цели, задачи, принципы и основные направления деятельности уполномоченных органов публичной власти, организаций и иных субъектов, принимающих участие в обеспечении информационно-психологической безопасности на основании законодательства Российской Федерации.

3. Правовую основу настоящей Концепции составляют Конституция Российской Федерации, Федеральный закон от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации», другие федеральные законы, Стратегия национальной безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации, Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, Основы государственной политики Российской Федерации в области международной информационной безопасности, Концепция информационной безопасности детей, другие документы стратегического планирования, иные нормативные правовые акты Российской Федерации, определяющие направления применения информационных и коммуникационных технологий в Российской Федерации.

4. Настоящая Концепция является основополагающим документом стратегического планирования, определяющим государственную политику

---

[1] Проект Концепции подготовлен старшим научным сотрудником сектора информационного права и международной информационной безопасности Института государства и права Российской академии наук, кандидатом юридических наук А.А. Смирновым.

в сфере обеспечения информационно-психологической безопасности, а также основой для конструктивного взаимодействия в этой сфере органов публичной власти и институтов гражданского общества, граждан Российской Федерации, иностранных граждан и лиц без гражданства.

5. Обеспечение информационной безопасности является одним из стратегических национальных приоритетов. Информационно-психологическая безопасность является составной частью системы информационной безопасности и представляет собой состояние защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия.

6. Российская Федерация при обеспечении информационно-психологической безопасности на долгосрочную перспективу исходит из необходимости постоянного совершенствования системы обеспечения информационно-психологической безопасности, а также политических, организационных, социально-экономических, информационных, правовых и иных мер:

а) по осуществлению мониторинга информационного пространства, выявлению, прогнозированию и оценке угроз информационно-психологической безопасности;

б) по реализации разработки и применению комплекса оперативных и долговременных мер по предупреждению и устранению угроз информационно-психологической безопасности, их локализации и нейтрализации последствий их проявления;

в) по созданию информационной среды доверия, повышению уровня цифровой грамотности и формированию культуры информационной безопасности;

г) по развитию частно-государственного партнерства и международного сотрудничества в области обеспечения информационно-психологической безопасности.

7. Для целей настоящей Концепции используются следующие основные понятия:

а) обеспечение информационно-психологической безопасности – деятельность по выработке и реализации системы правовых, организационных, информационных и иных мер, направленных на обеспечение защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия;

б) угроза информационно-психологической безопасности – фактор или совокупность факторов, способных причинить вред интересам личности, общества и государства посредством оказания деструктивного информационно-психологического воздействия;

в) деструктивное информационно-психологическое воздействие – негативное влияние на личность, социальные группы и общество деструктивной информации или коммуникации, а также сигналов от технических устройств, дистанционно воздействующих на психику человека через зрительные и слуховые сенсорные системы, создающее опасность причинения вреда интересам личности, общества и государства;

г) система обеспечения информационно-психологической безопасности – совокупность сил обеспечения информационно-психологической безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационно-психологической безопасности, а также правовых норм, регулирующих общественные отношения в сфере обеспечения информационно-психологической безопасности;

д) силы обеспечения информационно-психологической безопасности – государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационно-психологической безопасности;

е) средства обеспечения информационной безопасности – правовые, организационные, технические и другие средства, используемые силами обеспечения информационно-психологической безопасности;

ж) правовое обеспечение информационно-психологической безопасности – деятельность по разработке и реализации системы правовых средств, направленных на обеспечение защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия.

II. Основные угрозы информационно-психологической безопасности

8. Стремительное развитие информационно-коммуникационных технологий сопровождается ростом угроз безопасности, связанных с оказанием деструктивного информационно-психологического воздействия на личность, социальные группы и обществом в целом.

9. Расширяется использование информационно-коммуникационных технологий для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности, что представляет угрозу международному миру и безопасности. Активизируется деятельность специальных служб иностранных государств по проведению информационно-психологических операций в российском информационном пространстве.

10. В целях дестабилизации общественно-политической ситуации в Российской Федерации распространяется недостоверная общественно значимая информация, в том числе заведомо ложные сообщения об угрозе совершения террористических актов. Применяется тактика массовой рассылки ложных сообщений о минировании образовательных организаций и иных мест массового пребывания граждан, реализуемая с использованием современных средств связи и телекоммуникационных сетей. Новый потенциал для дезинформации открывают технологии искусственного интеллекта, в частности позволяющие создавать высококачественные подделки изображения и голоса человека (deepfakes).

11. Российские средства массовой информации и журналисты подвергаются в ряде зарубежных стран неприкрытому политическому давлению и цензуре, что грубо противоречит международно-правовым стандартам свободы массовой информации и демократии. При этом в западных массмедиа развязана мощная

скоординированная кампания очернения Российской Федерации, направленная на формирование негативного имиджа России в мире.

12. Доминирование транснациональных корпораций в интернет-секторе создает риски сбора большого массива персональных данных о российских пользователях и его применения для оказания таргетированного деструктивного информационно-психологического воздействия на отдельных людей и социальные группы. Используемые данными корпорациями подходы к модерации контента создают риски широкого распространения в сети Интернет противоправной информации, формирования искаженной картины событий, происходящих в России и в мире, навязывания негативных установок и ценностных ориентаций при одновременном блокировании возможности донесения альтернативных сведений. При этом ими систематически игнорируются законные требования российских властей об удалении или ограничении доступа к противоправному контенту, принятии иных мер по обеспечению информационно-психологической безопасности.

13. Традиционные российские духовно-нравственные и культурно-исторические ценности подвергаются активным нападкам со стороны западных государств и их союзников, транснациональных корпораций, иностранных некоммерческих неправительственных, религиозных, экстремистских и террористических организаций, а также поддерживающих их лиц и организаций внутри страны. При этом ими насаждаются социальные и моральные установки, противоречащие традициям, убеждениям и верованиям народов Российской Федерации.

14. Иностранными государствами и иными международными политическими акторами при поддержке и активном участии определенной внутренней прослойки населения проводится массированная кампания по фальсификации российской и мировой истории, искажению исторической правды и уничтожению исторической памяти, дискредитации российской культуры и русского языка, разжиганию межнациональных и межконфессиональных конфликтов, ослаблению государствообразующего народа.

15. Фактор анонимности в цифровой среде способствует широкому распространению негативного контента и ведению деструктивных коммуникаций, облегчает совершение преступлений и иных противоправных действий. В личностном плане ощущение анонимности обуславливает снятие ряда психологических барьеров в общении и поведении человека в информационном пространстве, что способствует проявлению им своих деструктивных наклонностей и интересов.

16. В сети Интернет размещаются материалы террористических и экстремистских организаций, призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, совершению самоубийства, осуществляется пропаганда криминального образа жизни, жестокости, насилия и иных антиобщественных действий, потребления наркотических средств и психотропных веществ, размещается иная противоправная информация. Основными объектами такого деструктивного воздействия являются дети и молодежь.

17. Возрастают масштабы мошенничеств, краж и иных преступлений, совершаемых с использованием информационно-коммуникационных технологий и приемов социальной инженерии. При этом способы и средства совершения таких преступлений становятся все изощреннее.

18. Широкое распространение в цифровой среде получили деструктивные молодежные субкультуры, содержащие негативные идеи, ценностные и поведенческие установки и нормы. Их продвижение осуществляется через многочисленные сообщества и каналы в социальных сетях и мессенджерах, в том числе при содействии спецслужб иностранных государств. Особую опасность представляют деструктивные субкультуры, провоцирующие совершение массовых убийств и применение иных актов насилия, а также суицид и иные формы аутодеструктивного поведения подростков.

19. Негативное воздействие на психику оказывают различные виды речевой агрессии и иной деструктивной коммуникации в социальных сетях

и мессенджерах, включая высмеивание (троллинг), травлю в сети (буллинг), доведение до самоубийства (буллицид) и др. Возможности Интернета также активно используются для склонения и иного вовлечения детей и молодежи в террористическую и экстремистскую деятельность, совершение преступлений, потребление и распространение наркотиков, иных антиобщественных действий или действий, представляющих опасность для жизни несовершеннолетнего.

20. Источником угроз информационно-психологической безопасности также выступают коммерческие компании, использующие сочетание продвинутых методов манипуляции сознанием потребителей и анализа их индивидуальной сетевой активности для агрессивного продвижения своих товаров и услуг.

21. Риски причинения вреда психическому и физическому здоровью граждан несут многочисленные «сетевые проповедники» и «учителя», распространяющие сомнительные, а иногда и откровенно ложные знания относительно здорового образа жизни, профилактики и лечения заболеваний, личностного роста, совершения юридически значимых действий и т.п. В период пандемии новой коронавирусной инфекции массированное распространение искаженной и фальсифицированной информации о заболевании, методах его предупреждения и лечения существенно снижает эффективность деятельности национальных систем здравоохранения и биологической безопасности.

22. В традиционных российских средствах массовой информации продолжает в большом объеме присутствовать информационная продукция, не способствующая духовному и моральному развитию личности и общества. При этом имеется существенный недостаток продукции, пропагандирующей традиционные духовно-нравственные ценности, позитивные ценностные и поведенческие установки, положительный образ настоящего и будущего России.

23. Источником угроз информационно-психологической безопасности для детей и иных уязвимых категорий населения являются компьютерные игры, содержащие натуралистичные сцены жесткого насилия, садизма, порнографии, обучающие потреблению наркотиков, изготовлению и применению в реальной жизни оружия и взрывных устройств, совершению террористических и иных

насильственных актов, а также самоубийств и иных аутодеструктивных действий. Особую опасность представляют игры в альтернативной реальности, предполагающие выполнение опасных игровых заданий офлайн.

24. Новые горизонты для деструктивного информационно-психологического воздействия на людей и социальные группы открывают системы виртуальной и дополненной реальности, использующие различные сенсорные каналы и создающие глубокий эффект погружения. Ставка крупных технологических компаний на развитие «метавселенных» позволяет прогнозировать их скорое появление и активное «погружение» в них населения, что создает комплекс новых рисков и вызовов.

25. Значимым фактором уязвимости для деструктивного информационно-психологического воздействия выступает низкий уровень медийной и цифровой грамотности населения и культуры информационной безопасности. Отмечается общественный запрос на усиление информационно-просветительской и образовательной деятельности в данной сфере, особенно среди детей и иных уязвимых слоев населения.

III. Национальные интересы в информационной сфере

26. Развитие глобального информационного общества и процессов цифровой трансформации оказывает влияние на все сферы общественной жизни и международные отношения. Информационно-коммуникационные технологии становятся мощным катализатором социального прогресса и одновременно генератором новых вызовов и угроз. Информационная сфера играет ключевую роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

27. Национальными интересами в информационной сфере (в части обеспечения информационно-психологической безопасности) являются:

а) обеспечение и защита конституционных прав и свобод человека и гражданина, включая право на свободу, неприкосновенность частной жизни, защиту

своей чести и доброго имени, свободу мысли и слова, право на информацию и свободу массовой информации;

б) формирование среды доверия в цифровой среде;

в) обеспечение доступа к информации, способствующей развитию личности и общества;

г) защита личности, социальных групп и общества в целом от деструктивного информационно-психологического воздействия;

д) гарантирование психического здоровья и благополучия граждан;

е) сохранение традиционных духовно-нравственных ценностей и национальной идентичности российского общества, повышение культурного потенциала страны;

ж) укрепление национального согласия, политической и социальной стабильности;

з) обеспечение информационного суверенитета России;

и) улучшение имиджа России и повышение ее авторитета на международной арене, усиление политического и культурного влияния России в мире;

к) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам деструктивного ИПВ на личность, социальные группы и общество.

28. Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации, создание условий для реализации прав и свобод человека и гражданина, стабильного социально-экономического развития страны и обеспечения ее национальной безопасности.

IV. Цели, задачи и принципы обеспечения информационно-психологической безопасности

29. Стратегической целью обеспечения информационно-психологической безопасности выступает поддержание состояния защищенности личности,

социальных групп и общества от деструктивного информационно-психологического воздействия, обеспечивающего гарантированную реализацию национальных интересов России.

30. Основными объектами деструктивного информационно-психологического воздействия являются:

- личность, большие и малые социальные группы, общество в целом;

- психика человека, включающая сознание и бессознательное, и групповые психические структуры, состоящие из группового (общественного) сознания и коллективного бессознательного;

- индивидуальные и групповые психические процессы (восприятие, память, мышление, мотивация и т.д.) и психические образования (образы, эмоции, цели, установки, архетипы и т.д.).

Приоритетным объектом правовой защиты от деструктивного информационно-психологического воздействия на макросоциальном уровне выступают дети.

31. Задачами обеспечения информационно-психологической безопасности являются:

а) прогнозирование, выявление, анализ и оценка угроз информационно-психологической безопасности;

б) анализ и оценка уязвимости личности, социальных групп и общества от деструктивного информационно-психологического воздействия;

в) стратегическое планирование в сфере обеспечения информационно-психологической безопасности;

г) правовое регулирование отношений в сфере обеспечения информационно-психологической безопасности;

д) применение комплекса оперативных и долговременных мер по профилактике, предупреждению, пресечению и устранению угроз информационно-психологической безопасности, минимизации и (или) ликвидации последствий их воздействия;

е) применение комплекса оперативных и долговременных мер по повышению способности личности, социальных групп и общества противостоять деструктивному информационно-психологическому воздействию;

ж) организация деятельности системы обеспечения информационно-психологической безопасности;

з) кадровое, информационное, материально-техническое и финансовое обеспечение деятельности субъектов обеспечения информационно-психологической безопасности;

и) международное сотрудничество в области обеспечения информационно-психологической безопасности.

32. Деятельность по обеспечению информационно-психологической безопасности осуществляется на основе следующих принципов:

а) соблюдение прав и свобод человека и гражданина;

б) гарантирование свободы массовой информации и запрет цензуры;

в) законность;

г) допустимость ограничения прав и свобод человека и гражданина в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;

д) суверенитет России в информационном пространстве;

е) создание условий, способствующих всестороннему духовному, нравственному, интеллектуальному и физическому развитию детей, воспитанию в них патриотизма, гражданственности и уважения к старшим;

ж) охрана исторической памяти и защита исторической правды;

з) системность и комплексность применения правовых, организационных, информационных и иных мер обеспечения информационно-психологической безопасности;

и) приоритет предупредительных мер обеспечения информационно-психологической безопасности;

к) частно-государственное партнерство и международное сотрудничество в обеспечении информационно-психологической безопасности.

V. Основные направления деятельности по обеспечению общественной безопасности

33. Деятельность по обеспечению информационно-психологической безопасности включает:

а) противодействие источникам угроз информационно-психологической безопасности;

б) блокирование или ослабление деструктивного информационно-психологического воздействия угроз на объекты информационно-психологической безопасности, включая ликвидацию (минимизацию) его последствий;

в) повышение жизнестойкости объектов информационно-психологической безопасности;

г) воздействие на факторы внешней информационной среды.

34. Основными направлениями деятельности по выработке и реализации государственной политики обеспечения информационно-психологической безопасности являются:

а) стратегическое планирование в сфере обеспечения информационно-психологической безопасности;

б) правовое регулирование в сфере обеспечения информационно-психологической безопасности;

в) осуществление государственного контроля (надзора) в сфере обеспечения информационно-психологической безопасности;

г) оказание государственных услуг в сфере обеспечения информационно-психологической безопасности;

д) координация деятельности субъектов обеспечения информационно-психологической безопасности;

е) организация материально-технического, финансового и информационного обеспечения деятельности субъектов обеспечения информационно-психологической безопасности;

ж) проведение научных исследований в области обеспечения информационно-психологической безопасности;

з) подготовка кадров в области обеспечения информационно-психологической безопасности;

и) осуществление международного сотрудничества в области информационно-психологической безопасности.

35. Основными направлениями деятельности по непосредственному обеспечению информационно-психологической безопасности выступают:

а) прогнозирование, выявление, анализ и оценка угроз информационно-психологической безопасности;

б) противодействие распространению негативной информации в средствах массовой информации и сети Интернет;

в) противодействие террористической и экстремистской пропаганде и вербовочной деятельности, разжиганию национальной, расовой, религиозной или социальной ненависти и вражды;

г) противодействие деструктивному информационно-психологическому воздействию со стороны государственных органов и специальных служб иностранных государств, иностранных и международных организаций;

д) обеспечение информационно-психологической безопасности детей;

е) защита чести, достоинства и деловой репутации гражданина, деловой репутации юридического лица;

ж) защита органов публичной власти, должностных лиц от деструктивного информационно-психологического воздействия;

з) противодействие фальсификации отечественной и мировой истории в ущерб интересам России;

и) противодействие распространению деструктивных субкультур и иных форм негативного информационно-психологического воздействия в духовной сфере;

к) противодействие преступлениям и административным правонарушениям, связанным с оказанием деструктивного информационно-психологического воздействия;

л) информирование российской и зарубежной общественности о внутренней и внешней политике Российской Федерации, ее официальной позиции по социально значимым событиям внутренней и международной жизни;

м) ведение контрпропаганды в России и за рубежом;

н) формирование цифровой грамотности граждан и культуры информационной безопасности.

VI. Организационные основы обеспечения информационно-психологической безопасности

36. Система обеспечения информационно-психологической безопасности является частью системы обеспечения информационной и национальной безопасности Российской Федерации.

Обеспечение информационно-психологической безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

37. Система обеспечения информационно-психологической безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

38. Состав системы обеспечения информационно-психологической безопасности определяется Президентом Российской Федерации.

39. Организационную основу системы обеспечения информационно-психологической безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет безопасности Российской Федерации, федеральные органы исполнительной власти, Генеральная прокуратура Российской Федерации, Следственный комитет Российской Федерации, Центральный банк Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационно-психологической безопасности.

Участниками системы обеспечения информационно-психологической безопасности являются: средства массовой информации и массовых коммуникаций, операторы связи, операторы информационных систем и иные информационные посредники, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационно-психологической безопасности.

40. В целях прогнозирования, мониторинга и контроля ситуации в области информационно-психологической безопасности и координации деятельности органов публичной власти и негосударственных участников системы обеспечения информационно-психологической безопасности создается государственная

система реагирования на информационно-психологические угрозы, представляющая собой единый централизованный комплекс, включающий силы и средства обнаружения, предупреждения, нейтрализации и ликвидации последствий воздействия информационно-психологических угроз. Положение о государственной системе реагирования на информационно-психологические угрозы утверждается Президентом Российской Федерации.

41. Реализация настоящей Концепции осуществляется на основе отраслевых документов стратегического планирования Российской Федерации. В целях актуализации таких документов Советом безопасности Российской Федерации определяется перечень приоритетных направлений обеспечения информационно-психологической безопасности на среднесрочную перспективу с учетом положений стратегического прогноза Российской Федерации.

42. Результаты мониторинга реализации настоящей Концепции отражаются в ежегодном докладе Секретаря Совета безопасности Российской Федерации Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению.