Первая редакция Доктрины увидела свет в 2000 году. Она создавалась на волне завершения 2-й Чеченской войны, повышенной террористической опасности, конфликта с НТВ, ведущим телеканалом России, категорически отказывающимся поддерживать государственную политику. В итоге в документ, посвященный обеспечению информационной безопасности, попали угрозы, релевантные обстановке.

Через 16 лет новую редакцию документа, посвященного вопросам информационной безопасности РФ, разработал Совет Безопасности. Она была утверждена указом президента 5 декабря 2016 года и уже на следующий день после подписания вступила в силу. Цифровая реальность в ней рассматривается уже как пространство, в котором происходит большинство коммуникаций, управленческих воздействий и финансовых трансакций.

Интересы России

Существенную часть документа занимает подробное перечисление интересов стран в цифровом мире.
Среди основных положений Доктрины, освещающих государственные интересы, названы:

- защита прав и свобод личности от любых посягательств, осуществляемых с использованием информационных средств, в том числе от попыток нарушить неприкосновенность частной жизни, от покушений на имущество, выраженное в электронной форме (безналичные средства на банковских картах), безопасность персональных данных;
- обеспечение защиты и неприкосновенности критических объектов информационной инфраструктуры от любых видов посягательств, совершаемых с использованием информационного оружия;
- защита финансовой сферы от любых информационных нападений, обеспечение устойчивого экономического развития, снижение уровня любых угроз, направленных на подрыв экономической стабильности;
- создание суверенного Рунета и усиление контроля над российским сектором Интернета. Эксперты в момент принятия Доктрины отметили, что эта идея труднореализуема, так как противоречит трансграничной концепции мировой информационной сети, тем не менее законопроект о суверенном Рунете готовится правительством;
- полная автаркия в области создания программного обеспечения, направленного на защиту информационной безопасности, а также комплектующих для электронной промышленности.

Угрозы

В документе названы типы угроз информационной безопасности, которые были выявлены Совбезом в ходе подготовки концепции.

В рамках изменившегося мира документ описывает следующие угрозы:

- стремление правительств некоторых стран использовать преимущество в сфере информационных технологий для организации нападений на объекты критической инфраструктуры РФ, причем такие нападения носят отчетливо военно-политический характер;
- воздействие на международную политику со стороны иностранной разведки с помощью информационно-психологического давления на граждан Российской Федерации, направленного на подрыв суверенитета, внутренней стабильности, инициацию и эскалацию религиозных и этнических конфликтов;
- подрыв репутации страны на международной арене, ее сознательное ухудшение, воспрепятствование деятельности российских информационных агентств и СМИ за рубежом.

Цели принятия Доктрины

Разработчики назвали цели, достижение которых предусмотрено в Доктрине. Они носят не только информационный характер, каждая из них является глобальной, состоящей из нескольких релевантных подцелей.

- влияние на международную информационную безопасность путем участия в разработке и принятии основополагающих международно-правовых документов;
- исключение возможности посягательства на информационную инфраструктуру, обеспечивающую управление технологическими и производственными процессами. Попытки перехвата управления крупными предприятиями, авария на которых способна привести как минимум к экологическим проблемам, уже зафиксированы. Задача защиты этой сферы от атак решается принятием закона о критических объектах инфраструктуры и разработок методологических рекомендаций, утвержденных приказами ФСТЭК РФ, которые призваны установить технические и организационные меры, используемые для защиты;
- бесперебойное функционирование всех объектов информационной инфраструктуры, а также объектов энергогенерации. Возможность оказаться без связи или электричества способна подорвать устойчивость экономики;

- контроль облика России в глазах международного сообщества, возможность влиять на международную информационную политику. В рамках этой цели лежит подцель доведения до международного сообщества достоверной и полной информации о позиции России по всем вопросам, касающимся мировой безопасности и социально-экономического развития. Здесь необходимо преодолеть противодействие, оказываемое работе за рубежом российских СМИ, например, Russia Today. Внутри страны эта цель выражается в стремлении понимать, что происходит в СМИ, в системе надзора за новостными агрегаторами, и в принятии закона о противодействии фейковым новостям;
- развитие отрасли производства цифровой техники и программного обеспечения, достижение полного импортозамещения в этой сфере, полная национальная независимость в этих ключевых отраслях;
- развитие науки и кадрового потенциала в сфере информационных технологий. Уже сейчас необходимо создать более миллиона рабочих мест для квалифицированных специалистов в области IT-технологий.

Международный аспект

Несмотря на то, что использование информационных средств в сфере международного права и геополитики не выделено в специальный раздел, этому вопросу посвящены многие положения Доктрины.

Документ включает следующие основные положения:

- современные угрозы, возникающие в информационной сфере, несовместимы с обеспечением мировой безопасности, причем реализуются они не только в военной, но и социальной и экономической сферах;
- необходимость создания единого информационного пространства, в котором все государства могли бы свободно взаимодействовать в рамках защиты своих и общих интересов, прав и свобод человека;
- потребность в правовой регламентации сферы международной информационной безопасности и проводимых в ней научных исследований;
- признание, что деятельность всех государств в едином информационном пространстве должна быть нацелена только на общемировое социально-экономическое развитие.