Проект

Для рассмотрения на совещании рабочей группы
5 октября 2015 г.

Доктрина информационной безопасности Российской Федерации

I. Общие положения

1. Доктрина информационной безопасности Российской Федерации (далее – Доктрина) представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

2. В Доктрине на основе анализа угроз и оценки состояния информационной безопасности Российской Федерации сформулированы основные направления обеспечения национальных интересов в информационной сфере с позиции реализации стратегических национальных приоритетов.

3. Доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором учитываются положения Стратегии национальной безопасности Российской Федерации, а также положения других документов стратегического планирования в Российской Федерации в сфере обеспечения национальной безопасности.

4. Доктрина служит основой для выработки мер по развитию системы информационной безопасности Российской Федерации, разработки и исполнения государственных программ в области информационной безопасности, а также организации сотрудничества Российской Федерации с другими государствами и международными институтами в области обеспечения информационной безопасности.

5. Правовую основу Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права и международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

6. В Доктрине используются следующие основные понятия:

а) информационная сфера – совокупность информации,

информационной инфраструктуры, субъектов, деятельность, которых связана с информационными и коммуникационными технологиями, а также механизмов регулирования возникающих при этом общественных отношений;

б) национальные интересы в информационной сфере – совокупность потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства в части, касающейся информационной сферы;

в) информационная безопасность Российской Федерации – состояние защищенности личности, общества и государства от внутренних и внешних угроз в информационной сфере, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства;

г) обеспечение информационной безопасности Российской Федерации – реализация взаимоувязанных нормативных правовых, организационных, оперативно-розыскных, разведывательных, научно-технических, информационно-аналитических, кадровых и экономических мер по прогнозированию, предупреждению, обнаружению и ликвидации последствий реализации угроз информационной безопасности Российской Федерации;

д) система информационной безопасности Российской Федерации – совокупность сил, осуществляющих скоординированную и спланированную деятельность по обеспечению информационной безопасности Российской Федерации, и используемых ими средств;

е) силы обеспечения информационной безопасности Российской Федерации – органы государственной власти, подразделения и должностные лица государственных органов и организаций различных форм собственности, решающие в соответствии с законодательством Российской Федерации задачи по обеспечению информационной безопасности Российской Федерации;

ж) средства обеспечения информационной безопасности Российской Федерации – технические и организационные средства, используемые силами обеспечения информационной безопасности Российской Федерации;

з) глобальное информационное пространство – среда трансграничного обращения информации, представляющее совокупность информационной инфраструктуры, информационных и коммуникационных технологий и собственно информации;

и) национальный суверенитет в глобальном информационном пространстве – способность государства проводить самостоятельную и независимую политику в глобальном информационном пространстве для защиты национальных интересов в информационной сфере;

к) информационные ресурсы Российской Федерации – информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом;

л) информационная инфраструктура Российской Федерации – совокупность информационных ресурсов Российской Федерации, включая критическую информационную инфраструктуру Российской Федерации и единую сеть электросвязи Российской Федерации;

м) информационные и коммуникационные технологии - процессы, методы и способы поиска, сбора, хранения, обработки, предоставления, распространения информации, осуществляемые с применением средств вычислительной техники и средств телекоммуникации;

II. Национальные интересы в информационной сфере

7. Информационные и коммуникационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное использование является фактором ускорения экономического развития и способствует формированию общества знания.

Информационная сфера играет важную роль в обеспечении политической стабильности в стране, обороны и безопасности государства, поддержания правопорядка, а также в укреплении равноправного стратегического партнерства.

8. Национальными интересами в информационной сфере являются:

а) соблюдение конституционных прав и свобод человека и гражданина в области получения и использования информации, включая неприкосновенность частной жизни при использовании информационных и коммуникационных технологий, информационную поддержку участия граждан в управлении государством, в политической жизни общества, а также сохранение и укрепление культурных, исторических и духовно- нравственных ценностей многонационального народа Российской Федерации;

б) развитие отрасли информационных технологий в Российской Федерации, включая разработку и производство средств обеспечения информационной безопасности, путем повышения конкурентоспособности продукции и услуг это отрасли на международном уровне и обеспечения их широкого использования в Российской Федерации, формирование в Российской Федерации общества знаний;

в) обеспечение устойчивого развития и бесперебойного функционирования информационной инфраструктуры Российской Федерации в мирное время, в период непосредственной угрозы агрессии и в военное время;

г) обеспечение доведения до российской и международной общественности достоверной информации о государственной политике Российской Федерации и об официальной позиции российского руководства по социально значимым событиям российской и международной жизни, содействие распространению духовных и культурных ценностей народов России по всему миру;

д) содействие формированию международного правового режима, нацеленного на противодействие угрозам стратегической стабильности, укрепление равноправного стратегического партнерства в области информационной безопасности и обеспечение национального суверенитета Российской Федерации в глобальном информационном пространстве.

III. Современное состояние информационной безопасности Российской Федерации

9. Информационные и коммуникационные технологии не только позитивно влияют на развитие экономики и совершенствование функционирования общественных и государственных институтов, но

и порождают новые вызовы и угрозы национальной безопасности. Это обусловлено тенденцией к использованию информационного пространства для решения военно-политических задач, а также в террористических и иных противоправных целях.

В результате реализации этих угроз может быть нанесен серьезный ущерб национальным интересам Российской Федерации в информационной сфере.

10. Состояние информационной безопасности Российской Федерации характеризуется наращиванием зарубежными странами возможностей по использованию информационно-технических воздействий, в том числе путем воздействия на критическую информационную инфраструктуру Российской Федерации для достижения своих военных и политических целей.

Усиливается ведение технической разведки в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

Милитаризация глобального информационного пространства и наращивание гонки информационных вооружений представляет серьезную угрозу международному миру, безопасности, глобальной и региональной стабильности.

11. Активизируется использование специальными службами и подконтрольными общественными организациями отдельных государств информационных и коммуникационных технологий в качестве инструмента информационно-психологических воздействий для подрыва суверенитета и нарушения территориальной целостности других государств, дестабилизации внутриполитической и социальной ситуации в различных регионах мира. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации и структуры.

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 широко используются механизмы воздействия на индивидуальное, групповое и общественное сознание.

Отмечается тенденция увеличения объема материалов в зарубежных средствах массовой информации, содержащих необъективную и предвзятую информацию о внешней и внутренней

политике Российской Федерации. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности.

Наращивается информационное воздействие на население страны, в первую очередь на молодежь, с целью размывания культурных и духовных ценностей, подрыва нравственных устоев, исторических основ и патриотических традиций.

12. Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число инцидентов, связанных с нарушением законных прав граждан на неприкосновенность частной жизни, личной и семейной тайны при использовании информационных и коммуникационных технологий.

Недостаточный уровень защищенности информационных систем государственных органов и организаций различных форм собственности и сетей связи в условиях трансграничности и анонимности глобального информационного пространства является одним из основных факторов, способствующих активизации такой противоправной деятельности.

13. В экономической области сохраняется отставание Российской Федерации от ведущих зарубежных государств в создании конкурентоспособных информационных и коммуникационных технологий и продукции на их основе (в том числе суперкомпьютеров и электронной компонентной базы), что обуславливает зависимость Российской Федерации от экспортной политики зарубежных стран.

При этом, как правило, внедрение информационных и коммуникационных технологий не увязано с обеспечением информационной безопасности.

Отсутствует единая государственная организационно-техническая политика по обеспечению в мирное время, в период непосредственной угрозы агрессии и в военное время устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации.

14. Негативно сказывается на развитии международных отношений стремление отдельных государств для достижения экономического и геополитического преимущества использовать технологическое доминирование в глобальном информационном

пространстве, в том числе путем оказания влияния на развитие и функционирование национальных сегментов.

Отсутствие институтов международного права, регулирующих между государствами отношения в глобальном информационном пространстве, включая кризисные ситуации, с учетом специфики использования информационных и коммуникационных технологий, препятствует формированию системы международной информационной безопасности, как гаранта стратегической стабильности и равноправного стратегического партнерства в мире.

IV. Основные направления обеспечения информационной безопасности Российской Федерации

15. Защита национальных интересов в информационной сфере обеспечивается с позиции реализации стратегических национальных приоритетов на основе консолидации усилий государственных структур, общественных организаций и граждан, общества и государства.

16. Деятельность государственных органов в сфере обеспечения информационной безопасности Российской Федерации основывается на следующих принципах:

соблюдение баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации в целях обеспечения информационной безопасности;

правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

открытость в реализации функций органов государственной власти Российской Федерации, предусматривающей информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;

соблюдение общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации.

17. Обеспечение информационной безопасности Российской Федерации в области национальной обороны направлено:

на содействие созданию международно-правовых условий, обеспечивающих снижение риска использования информационно-коммуникационных технологий для осуществления враждебных действий и актов агрессий;

на систематическое выявление угроз информационной безопасности в военной сфере и их источников;

на развитие военной политики в области информационной безопасности Российской Федерации;

на совершенствование системы информационной безопасности Вооруженных Сил Российской Федерации, других войск и органов;

на поддержание устойчивого функционирования и безопасного использования единого информационного пространства Вооруженных Сил Российской Федерации;

на развитие сил и средств информационного противоборства;

на осуществление стратегического сдерживания и предотвращение военных конфликтов в информационном пространстве в целях обеспечения обороны и безопасности Российской Федерации, а также ее союзников;

на противодействие деятельности по информационному воздействию на население и в первую очередь на молодых граждан страны, имеющей целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества

18. Обеспечение информационной безопасности Российской Федерации в области государственной и общественной безопасности направлено:

на повышение защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак и устойчивости ее функционирования, включая совершенствование механизмов предупреждения и обнаружения компьютерных атак и ликвидации последствий их проведения;

на противодействие разведывательной и иной деятельности специальных служб и организаций иностранных государств, а также отдельных лиц, направленной на нанесение ущерба обеспечению информационной безопасности Российской Федерации в различных областях жизнедеятельности;

на повышение эффективности профилактики и противодействия правонарушениям в сфере компьютерной информации;

на противодействие использованию информационных и коммуникационных технологий в целях пропаганды идеологии терроризма и распространения идей экстремизма, ксенофобии, национальной исключительности, направленных на подрыв общественно-политической стабильности, насильственное изменение основ конституционного строя Российской Федерации, нарушения ее единства и территориальной целостности, а также для призывов к осуществлению иных противоправных деяний;

на предотвращение попыток иностранного контроля информационной инфраструктуры Российской Федерации путем введения мер законодательного, организационного и экономического характера;

на создание, развитие и обеспечение функционирования защищенных информационных систем, ситуационных центров и сетей связи, предназначенных для нужд обороны и безопасности страны, поддержания правопорядка, гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, реализации иных полномочий государственных органов, информационно-технического и информационно-аналитического обеспечения их деятельности;

на обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию;

на противодействие использованию специальными службами и организациями иностранных государств средств и методов информационного противоборства с целью нанесения ущерба государственной и общественной безопасности Российской Федерации;

на содействие созданию международно-правовых условий, обеспечивающих снижение риска использования информационно-коммуникационных технологий в террористических, экстремистских и криминальных целях.

19. Обеспечение информационной безопасности Российской Федерации в экономической области направлено:

на создание конкурентоспособной и вносящей существенный вклад в формирование валового внутреннего продукта страны отечественной индустрии информационных и коммуникационных технологий, средств вычислительной техники, радиоэлектроники, телекоммуникационного оборудования и программного обеспечения, отечественной электронной промышленности;

на создание, развитие и широкое внедрение конкурентоспособных на мировом уровне отечественных информационных и коммуникационных технологий и продукции на их основе, включая суперкомпьютерные технологии и перспективные средства обеспечения информационной безопасности;

на развитие отечественных конкурентоспособных электронной компонентной базы и микроэлектронных технологий, обеспечение потребности внутреннего рынка в такой продукции и выхода этой продукции на мировой рынок;

на использование информационных и коммуникационных технологий для развития экономики Российской Федерации, включая расширение участия России в международной кооперации производителей этих средств и систем;

на повышение информационной безопасности национальной платежной системы, защищенности информационных систем других секторов экономики.

20. Обеспечение информационной безопасности Российской Федерации в области науки, технологий и образования направлено на развитие научных и научно-технологических направлений, способных обеспечить конкурентные преимущества национальной отрасли информационных технологий, на повышение уровня общего и профессионального образования населения страны в области информационных и коммуникационных технологий и информационной безопасности.

21. Обеспечение информационной безопасности Российской Федерации в области стратегической стабильности и равноправного стратегического партнерства реализуется на основе формирования системы международной информационной безопасности, обеспечивающей эффективное противодействие использованию информационно-коммуникационных технологий в агрессивных, террористических, экстремистских, криминальных целях, а также

способствующей поддержанию национального суверенитета Российской Федерации в глобальном информационном пространстве.

22. Общими направлениями обеспечения информационной безопасности Российской Федерации являются:

информационное обеспечение государственной политики Российской Федерации;

защита информации, обрабатываемой в государственных органах и органах местного самоуправления, а также организациях различных форм собственности;

подготовка, переподготовка и повышение квалификации кадров в области информационной безопасности;

формирование культуры информационной безопасности граждан Российской Федерации;

обеспечение устойчивого и безопасного функционирования единой сети электросвязи Российской Федерации.

23. Повышение эффективности информационного обеспечения государственной политики Российской Федерации основано:

на противодействии негативному влиянию зарубежных информационных структур на духовную, экономическую и политическую сферы общественной жизни Российской Федерации путем навязывания нетрадиционных для России моральных и нравственных ценностей;

на противодействии политики отдельных зарубежных государств по ограничению деятельности российских средств массовой информации на их территории;

на укреплении российских средств массовой информации, в том числе путем расширения их возможностей по увеличению аудитории и своевременному доведению до граждан объективной информации;

на совершенствовании системы профессиональной подготовки и повышения квалификации журналистских кадров;

на проведении единой скоординированной информационной политики российскими государственными средствами массовой информации, информационными ресурсами и структурами органов государственной власти по взаимодействию со средствами массовой информации и общественностью;

на развитии сети российских неправительственных организаций для использования потенциала общественной дипломатии в целях информационной поддержки внешней политики России за рубежом;

на расширении возможности взаимодействия российских неправительственных организаций со структурами гражданского общества зарубежных стран;

на задействовании потенциала неправительственных организаций российских соотечественников, проживающих за рубежом, для реализации проектов по защите национальных интересов в информационной сфере.

24. Повышение уровня защиты информации, обрабатываемой в государственных органах и органах местного самоуправления, а также организациях различных форм собственности основано:

на развитии производства отечественных конкурентоспособных средств и систем информатизации, телекоммуникации и защиты информации, расширение участия России в международной кооперации производителей этих средств и систем;

на совершенствовании методов, способов и средств защиты информации, оценки реальной защищенности информационных систем и информационно-телекоммуникационных сетей, развитии форм их использования;

на определении в органах государственной власти и органах местного самоуправления, организациях различных форм собственности должностных лиц и подразделений, ответственных за обеспечение информационной безопасности, включая защиту государственной тайны, защиту от иностранных технических разведок и техническую защиту информации, и повышении уровня организационно-штатного обеспечения и оснащенности этих подразделений;

на организации обмена между государством, обществом и гражданами информацией об уязвимостях информационных и коммуникационных технологий, методах и средствах осуществления компьютерных атак и компьютерных инцидентах;

на развитии и широком применении сертифицированных средств криптографической защиты информации, защищенных информационных систем и сетей связи, технических средств и оборудования, а также проведении специальных работ, направленных на обеспечение соответствия технических средств, оборудования и категорированных помещений предъявляемым требованиям по безопасности информации;

на развитии и активном внедрении нормативной правовой и методической базы защиты информации, включая стандарты и спецификации, регулирующие вопросы защиты информации при использовании различных информационных и коммуникационных технологий;

на взаимоувязывание на нормативном правовом и организационном уровне мероприятий по внедрению информационных и коммуникационных технологий с мероприятиями по обеспечению информационной безопасности;

на сертификации средств защиты информации и контроля эффективности их использования, а также аттестации объектов информатизации по требованиям безопасности информации;

на развитии форм и методов саморегулирования деятельности в области на этом направлении, а также внедрении механизмов государственно-частного партнерства;

на введение законных ограничений в режимах использования технических средств, подлежащих защите.

25. Развитие системы подготовки, переподготовки и повышения квалификации кадров в области информационной безопасности основано:

на централизации управления системой профессионального образования и повышения кадрового потенциала в области обеспечения информационной безопасности;

на совершенствовании федерального государственного контроля качества образования при реализации основных профессиональных образовательных программ в области обеспечения информационной безопасности;

на задействовании механизмов целевого финансирования образовательных учреждений, осуществляющих подготовку кадров в области информационной безопасности;

на формировании единых (национальных, межведомственных, отраслевых) подходов к подготовке и переподготовке кадров в области информационной безопасности;

на привлечении талантливой молодежи в сферу информационной безопасности, в том числе за счет повышение престижа и привлекательности специальностей в области обеспечения информационной безопасности;

на поддержании на высоком научно-техническом уровне технологической и методологической базы обучения в области информационной безопасности, включая внедрение современной учебно-лабораторной базы и стендовых полигонов;

на повышении качества фундаментального образования в базовых научно-технических дисциплинах, в первую очередь – в части физико-математических наук, и повышения уровня образования в прикладных областях информационной безопасности.

26. Формирование культуры информационной безопасности личности нацелено на создание условий для обеспечения защищенности личности от угроз различного характера при использовании информационных и коммуникационных технологий посредством совершенствования знаний, умений, навыков, компетенций, способностей, а также за счет повышения правосознания граждан Российской Федерации. Достижению этой цели будет способствовать решение следующих основных задач:

создание, развитие и распространение научно и/или практически обоснованных рекомендаций, правил, учебно-методических и просветительских материалов по вопросам безопасного использования информационных и коммуникационных технологий, в том числе для малообеспеченных и социально незащищенных, а также пожилых граждан;

проведение образовательной, культурно-просветительской и профилактической работы среди всех категорий пользователей информационных и коммуникационных технологий в целях формирования культуры информационной безопасности личности;

создание, обеспечение функционирования и развитие системы информационно-консультативной, технологической и технической помощи по обнаружению, предупреждению и ликвидации последствий проявления угроз информационной безопасности личности;

развитие нормативного правового регулирования отношений в области формирования культуры информационной безопасности личности, а также формирование и развитие правосознания и ответственного отношения граждан к вопросам использования информационных и коммуникационных технологий.

27. Обеспечение устойчивого и безопасного функционирования единой сети электросвязи Российской Федерации основано:

на централизации мониторинга функционирования и управления единой сети электросвязи Российской Федерации;

на построении сетей связи с учетом требований по устойчивости и безопасности их функционирования;

на повышении оперативности восстановления единой сети электросвязи Российской Федерации в условиях чрезвычайных ситуаций и в военное время;

на преимущественном использовании в сетях связи отечественного телекоммуникационного оборудования и средств управления.

V. Организационные основы обеспечения информационной безопасности Российской Федерации

28. Система информационной безопасности Российской Федерации является составной частью системы обеспечения национальной безопасности.

29. В рамках обеспечения функционирования системы информационной безопасности органы государственной власти решают следующие задачи:

мониторинг и оценка состояния информационной безопасности Российской Федерации, прогнозирование и выявление источников угроз информационной безопасности, определение приоритетных направлений предотвращения и нейтрализации этих угроз;

планирование и проведение комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации;

развитие и координация взаимодействия сил и средств обеспечения информационной безопасности Российской Федерации;

совершенствование законодательного, нормативного правового, организационного, оперативно-розыскного, разведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения информационной безопасности Российской Федерации;

обеспечение реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;

проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;

организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации.

30. Система информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, с учетом предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, определяемых законодательством Российской Федерации в области безопасности.

31. Президент Российской Федерации определяет систему информационной безопасности Российской Федерации, приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации, а также меры по реализации Доктрины.

32. Основными субъектами организационной основы системы информационной безопасности Российской Федерации являются: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, межведомственные и государственные комиссии, 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 обеспечения информационной безопасности Российской Федерации.

Участниками системы информационной безопасности Российской Федерации являются собственники элементов критической информационной инфраструктуры Российской Федерации и эксплуатирующие эти элементы организации различных форм собственности, средства массовой информации и массовой коммуникации, операторы связи, операторы информационных систем, обладатели информации, общественные объединения, а также

иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач обеспечения информационной безопасности.

33. Развитие и совершенствование системы информационной безопасности Российской Федерации достигается путем:

совершенствования форм и методов взаимодействия сил и средств обеспечения информационной безопасности Российской Федерации в целях повышения их готовности к парированию угроз и оперативному реагированию на инциденты в информационной инфраструктуре Российской Федерации;

усиления вертикали и централизации управления силами и средствами информационной безопасности Российской Федерации на федеральном, межрегиональном, региональном и объектовом уровне;

совершенствования информационно-аналитического и научно-технического обеспечения функционирования системы информационной безопасности Российской Федерации;

повышения эффективности взаимодействия между государственными органами, органами местного самоуправления, организациями различных форм собственности и гражданами при решении задач в области информационной безопасности;

совершенствования механизмов планирования мероприятий в области обеспечения информационной безопасности Российской Федерации и оценки их эффективности.

34. Результаты мониторинга реализации Доктрины отражаются в ежегодном докладе Секретаря Совета Безопасности Российской Федерации Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению.

35. Контроль реализации Доктрины осуществляется Советом Безопасности Российской Федерации в порядке, определенном в положении о нем.