ГУАП

КАФЕДРА № 33

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

канд. техн. наук, доцент		В. А. Рындюк
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ

Законодательство в области информационной безопасности РФ

по курсу: Защита информации

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ гр. № 4131з		М. Д. Быстров
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2025

Задание

Сравнить Доктрины ИБ РФ 2000 и 2016гг по вопросам:

1. Назначение Доктрины (т.е. с какой целью она была создана)

2.Чьи интересы прописаны в Доктрине

3.Угрозы ИБ

4.Меры борьбы с угрозами (т.е. методы , средства, подходы.. и т.д.)

Работу выполнить в MS Word.

Введение

Доктрина информационной безопасности Российской Федерации – официальный документ, в современной редакции представляющий из себя «систему официальных взглядов на обеспечение национальной безопасности». Действующая редакция утверждена 5.12.2016 года. Предыдущая редакция была утверждена в 2000г. Необходимость разработки новой версии доктрины была объяснена в публикации Совбеза РФ (http://www.scrf.gov.ru/news/allnews/874/) следующим образом: «Актуализация подходов к защите национальных интересов в информационной сфере с учетом современных реалий станет основной проекта новой редакции Доктрины». Из этого следует, что доктрина 2000г была признана устаревшей.

В данной лабораторной работе будет произведено сравнение двух редакций доктрины в разных её аспектах согласно заданию.

1. Назначение Доктрины (т.е. с какой целью она была создана)

2000 г:

Настоящая Доктрина служит основой для:

формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;

подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

разработки целевых программ обеспечения информационной безопасности Российской Федерации.

2016г:

Настоящая Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

Настоящая Доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. N 683, а также других документов стратегического планирования в указанной сфере.

Настоящая Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

Сравнение

В документе 2000г одна из целей – создание основы для формирования государственной политики в сфере информационной безопасности. В то же время, в доктрине 2016 года указано, что в документе содержится описание определенных на основе проведенного анализа стратегических целей и основных направлений обеспечения информационной безопасности. Из этого можно заключить, что Доктрина 2016 года позиционируется как закрепленная документально официальная государственная позиция, которой можно руководствоваться при проведении конкретных мероприятий по обеспечению информационной безопасности. В то же время, Доктрина 2000 года является документом, на основе которого можно основывать законодательные инициативы и использовать его содержание для подготовки предложений по обеспечению ИБ.

Несмотря на сходство двух редакций документа в этом аспекте, новую редакцию возможно использовать более активно при проведении мероприятий по обеспечению ИБ, благодаря тому что в ней прописаны конкретные основные направления этой деятельности.

2.Чьи интересы прописаны в Доктрине

2000г:

Национальные интересы Российской Федерации в информационной сфере и их обеспечение

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной

стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

2016г:

национальные интересы Российской Федерации в информационной сфере (далее - национальные интересы в информационной сфере) - объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

8. Национальными интересами в информационной сфере являются:

а) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

9. Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Сравнение

В обоих документах упоминаются национальные интересы, состоящие из интересов личности, общества и государства. При раскрытии составляющих национальных интересов в Доктрине 2000 года в достаточной степени подробно раскрываются три упомянутых составляющих. В Доктрине 2016 года также раскрываются интересы личности, защищенные Конституцией РФ, но отдельно интересы общества и государства, как пункты, не раскрываются. В целом, описание национальных интересов в новой редакции структурно отличается от описания в старой редакции.

В старой редакции отдельно описаны составляющие национальных интересов по субъектам (интересантам), а затем отдельно описаны четыре предметные составляющие этих интересов (конкретные, прикладные цели).

В новой редакции нет описания национальных интересов с точки зрения субъектов, сразу приводится перечисление предметных составляющих национальных интересов. Таким образом, разделение национальных интересов на интересы личности, общества и государства остается только в виде перечисления. Национальные интересы представляются в новой редакции более консолидированными.

Также можно отметить некоторым образом связанную тенденцию: в старой редакции Конституция РФ упомянута 28 раз, чаще всего в контексте прав и свобод

гражданина, и даже в контексте ограничения полномочий Президента РФ: «Президент Российской Федерации руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности Российской Федерации» (п. 11). В новой же редакции Конституция РФ упомянута 8 раз.

3.Угрозы ИБ

2000г:

Виды угроз информационной безопасности Российской Федерации

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

угрозы информационному обеспечению государственной политики Российской Федерации;

угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

К внешним источникам относятся:

деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

обострение международной конкуренции за обладание информационными технологиями и ресурсами;

деятельность международных террористических организаций;

увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение

нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

критическое состояние отечественных отраслей промышленности;

неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

недостаточная экономическая мощь государства;

снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

2016г:

Основные информационные угрозы и состояние информационной безопасности

10. Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

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

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

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

Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности.

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

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

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

15. Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности.

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

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

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

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

Сравнение

Можно отметить, что структурно определение угроз ИБ также претерпело изменение. В документе 2000 года угрозы разделены на внешние и внутренние угрозы. В новой редакции подобного разделения нет.

За 16 лет, разделяющих два документа, уровень развития информационных технологий в мире заметно вырос. Уровень вовлеченности населения в информационное поле, которое в пределах государств слабо контролируется правительствами (больше всего это заметно на примере сети Интернет), привел к тому, что на государственном уровне вопрос о контроле этого информационного стал очень заметен. Даже в 2000 году, как можно заметить из Доктрины 2000 г., эта тенденция была заметна: «стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков». К 2016 году информатизация всех стран, а развивающихся, таких как Россия, особенно, кратно выросла. Поэтому эта тенденция информационных угроз из потенциально опасной стала критически важной в области внешней и внутренней политики: «возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности».

Таким образом, в Доктрине 2016 года признается, что эти угрозы являются неотъемлемой частью современной общественной жизни, в то время как в Доктрине 2000 года этот вопрос ещё не ставится так остро.

Также можно отметить, что в старой редакции упоминается упадочное состояние экономики: «недостаточная экономическая мощь государства» как одна угроз ИБ. В новой редакции не указывается на экономические проблемы общего характера. Это можно объяснить тем, что экономически Российская Федерация с 2000 года стала более конкурентноспособной, а в сфере информатизации общественной жизни (например, в банковской, транспортной, налоговой сферах и т.д.) сумела произвести впечатляющий скачок, поставивший страну по этому показателю наравне с ведущими экономиками мира. Также с 2000 года изменился «тон» официальных документов, и упоминание слабости экономики в документе, описывающем официальную позицию правительства, стало недопустимым. По этому пункту старая редакция явно устарела к 2016 году.

4.Меры борьбы с угрозами (т.е. методы , средства, подходы.. и т.д.)

2000г:

Общие методы обеспечения информационной безопасности Российской Федерации

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Наиболее важными направлениями этой деятельности являются:

внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации;

законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;

разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное

распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;

уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;

законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;

определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций;

создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности *Российской Федерации являются:*

создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;

усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;

формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности *Российской Федерации включают в себя:*

разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;

совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

2016г:

21. В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;

г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;

д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

23. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;

д) повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;

е) повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

ж) обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;

з) совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;

и) повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;

к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

23. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;

д) повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;

е) повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

ж) обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;

з) совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;

и) повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;

к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

25. Основными направлениями обеспечения информационной безопасности в экономической сфере являются:

а) инновационное развитие отрасли информационных технологий и электронной промышленности, увеличение доли продукции этой отрасли в валовом внутреннем продукте, в структуре экспорта страны;

б) ликвидация зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности за счет создания, развития и широкого внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе;

в) повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли информационных технологий и электронной промышленности, разработку, производство и эксплуатацию средств обеспечения информационной безопасности, оказывающих услуги в области обеспечения информационной безопасности, в том числе за счет создания благоприятных условий для осуществления деятельности на территории Российской Федерации;

г) развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов, обеспечение потребности внутреннего рынка в такой продукции и выхода этой продукции на мировой рынок.

27. Основными направлениями обеспечения информационной безопасности в области науки, технологий и образования являются:

а) достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения информационной безопасности;

б) создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

в) проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;

г) развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;

д) обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

29. Основными направлениями обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства являются:

а) защита суверенитета Российской Федерации в информационном пространстве посредством осуществления самостоятельной и независимой политики, направленной на реализацию национальных интересов в информационной сфере;

б) участие в формировании системы международной информационной безопасности, обеспечивающей эффективное противодействие использованию информационных технологий в военно-политических целях, противоречащих международному праву, а также в террористических, экстремистских, криминальных и иных противоправных целях;

в) создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;

г) продвижение в рамках деятельности международных организаций позиции Российской Федерации, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере;

д) развитие национальной системы управления российским сегментом сети "Интернет".

Сравнение

В Доктрине 2000 года методы обеспечения информационной безопасности разделены на три группы: правовые, организационно-технические и экономические. Меры разделены по типу, в этих группах они будут иметь принципиально разную форму: правовые меры будут утверждены законодательно, организационно-технические будут представлять собой автоматизацию различных сфер общественной жизни, экономические будут влиять на развитие сферы ИБ (распределение бюджета).

В редакции 2016 года термин «метод» не употребляется при перечислении мер по обеспечению ИБ, вместо него используется термин «направление обеспечения ИБ». Эти направления разделяются по различным областям:

- Область обороны страны
- Область государственной и общественной безопасности
- Экономическая сфера
- Область науки, технологий и образования
- Область стратегической стабильности и равноправного стратегического партнерства

В новой редакции меры разделены не по типу, а по их влиянию на конкретную сферу: какое именно влияние с точки зрения ИБ та или иная мера должна оказать.

Также стоит отметить, что в новом документе отдельное внимание уделяется информационной безопасности оборонной сферы, а также влиянию информационных угроз на население. В редакции 2000 года этому уделялось гораздо меньшее внимание.

Вывод

Было проведено сравнение двух редакции Доктрины информационной безопасности РФ в четырех аспектах:

1. Назначение Доктрины (т.е. с какой целью она была создана)

2.Чьи интересы прописаны в Доктрине

3.Угрозы ИБ

4.Меры борьбы с угрозами (т.е. методы , средства, подходы.. и т.д.)

Было выявлено, что оба документа имеют как сходства, так и различия.

К сходствам можно отнести: представление официальной позиции правительства РФ на проблемы ИБ, возможность использования документа для законодательной и иной деятельности, связанной со сферой информационной безопасности.

В то же время, документы отличаются объемом и структурой. На примере структурных различий видно, что новая редакция создавалась в условиях, когда проблемы ИБ стоят гораздо острее, чем при создании первой редакции документа.