Министерство образования науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

Тульский государственный университет

Институт прикладной математики и компьютерных наук

Кафедра

Информационная безопасность

**ПРАКТИЧЕСКАЯ РАБОТА №6**

по дисциплине

**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Выполнила:  
ст. гр. 230711, Павлова В.С. \_\_\_\_\_\_\_\_\_\_\_\_

Проверила:

к.т.н., доц. Баранова Е.М. \_\_\_\_\_\_\_\_\_\_\_\_

Тула, 2022 г.

**Практическая работа №6. Анализ доктрины ИБ РФ**

План анализа документа:

1. Номер, название, дата введения документа;
2. Состав (кол-во глав, разделов, статей, приложений и т.д.);
3. Название разделов или глав с описанием в них кол-ва статей/пунктов;
4. Выделение основной мысли по каждой главе или разделу;
5. Характеристика состава приложений;
6. Вывод.

Доктрина информационной безопасности Российской Федерации была утверждена [Указом](http://kremlin.ru/acts/news/53418) Президента Российской Федерации от 5 декабря 2016 г. №646. Документ создан на основе анализа угроз и оценки состояния ИБ РФ и развивает положения "Стратегии национальной безопасности РФ от 31 декабря 2015 года № 683 (ссылка на этот и последующие документы будут указаны в приложении).

Документ состоит из пяти частей, первая из которых называется «I. Общие положения» и содержит шесть пунктов (с 1-го по 6-ой), у второго из них – восемь подпунктов. Раздел содержит определения понятий, которыми оперирует текст Доктрины, к примеру, в нем уточняется, что под информационной безопасностью Российской Федерации подразумевается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Другой важный термин – угроза информационной безопасности Российской Федерации (иначе – информационная угроза), которая представляет из себя совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Также в этой части Доктрины разъясняется, что правовой основой документа являются Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, а также федеральные и нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации. 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.

Вторая часть документа «II. Национальные интересы Российской Федерации в информационной сфере» вносит ясность о постановке приоритетов государства, которая, как сказано в начале раздела, играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации. В разделе имеется три пункта (с 7-го по 9-ый), во втором из которых есть пять подпунктов. Все перечисленные в статье интересы преследуют одну глобальную цель – создание 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.

Третья часть документа называется «III. Основные информационные угрозы и состояние информационной безопасности» и содержит десять пунктов (с 10-го по 19-ый), в которых изложена информация о текущем состоянии информационной безопасности Российской Федерации в области экономики, науки, обороны и геополитики, а также причины появления информационных угроз и негативные факторах, влияющие на состояние информационной безопасности в различных сферах деятельности государства – от внешней политической до внутренней экономической. Среди них наиболее важными можно выделить наращивание рядом зарубежных стран возможностей информационно-технического воздействия и информационной инфраструктуры в военных целях, аферы в кредитно-финансовой сфере, увеличение масштабов компьютерных атак на объекты критической информационной инфраструктуры – в том числе сайтов вроде «Госуслуги» или «Доктор71.ру», которыми постоянно пользуются граждане.

Четвёртый раздел документа – «IV. Стратегические цели и основные направления обеспечения информационной безопасности» – содержит 10 пунктов (с 20 по 29-ый), несколько из которых имеют разделение на подпункты. Этот раздел как бы разделен на основные тематические направления, а подпункты поясняют, что конкретно необходимо для защиты информации и прав граждан в данной сфере. В них регламентируется:

а) деятельность по обеспечению информационной безопасности в области обороны страны – *сдерживание и предотвращение военных конфликтов, а также совершенствование системы обеспечения информационной безопасности*;

б) государственной и общественной безопасности – *противодействие пропаганде экстремистской идеологии, повышение защищенности критической информационной инфраструктуры, защита гостайны и нейтрализация разрушения духовно-нравственных ценностей*;

в) в сфере экономики – *импортозамещение в сфере информационных технологий и развитие отрасли информационных технологий*;

г) в сфере науки и технологий – *поддержка инновационного развития системы обеспечения информационной безопасности, отрасли информационных технологий*;

д) в области стратегической стабильности и равноправного стратегического партнерства – *формирование устойчивой системы неконфликтных межгосударственных отношений.*

Пятый и последний раздел – «V. Организационные основы обеспечения информационной безопасности» содержит девять пунктов (с 30-го по 38-ой), три из которых (34-36) имеют по несколько подпунктов. В этом разделе документа определяется, как именно осуществляется деятельность по защите информационной сферы. Как сказано в одном из пунктов, система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти. В разделе перечислен состав системы обеспечения безопасности, который определяется Президентом РФ и в который выходят такие государственные органы как Совет Федерации, государственная дума, правительство РФ,  Совет безопасности РФ, федеральные органы исполнительной власти, ЦБ и другие. Частью этой большой системы являются также собственники объектов критической информационной структуры, деятели СМИ, операторы информационных систем и другие.

Статья регламентирует полномочия и обязанности членов этой системы, принципы их деятельности и задачи, а также способ мониторинга реализации Доктрины –  ежегодный доклад Секретаря Совета Безопасности Российской Федерации Президенту. Принципиальной основой деятельности системы обеспечения безопасности и органов госструктур является соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности. Для этого необходимо своевременное прогнозирование и обнаружение информационных угроз, совершенствование технической составляющей информационных систем, улучшение взаимодействия государственных органов и всего, что обеспечивает защиту прав и свобод граждан, а также принадлежащей им информации. Приложений Доктрина не имеет.

*Вывод:*  в ходе изучения курса «Основы информационной безопасности» был рассмотрен и проанализирован документ «Доктрина информационной безопасности Российской Федерации» от 5 декабря 2016 г. №646. Также были выявлены ссылки на следующие документы: указ Президента Российской Федерации от 31.12.2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации».

Приложение:

1. Указ Президента Российской Федерации от 31.12.2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации»: http://www.kremlin.ru/acts/bank/40391