Лекция №2

Нормативно-правовые средства защиты информации.

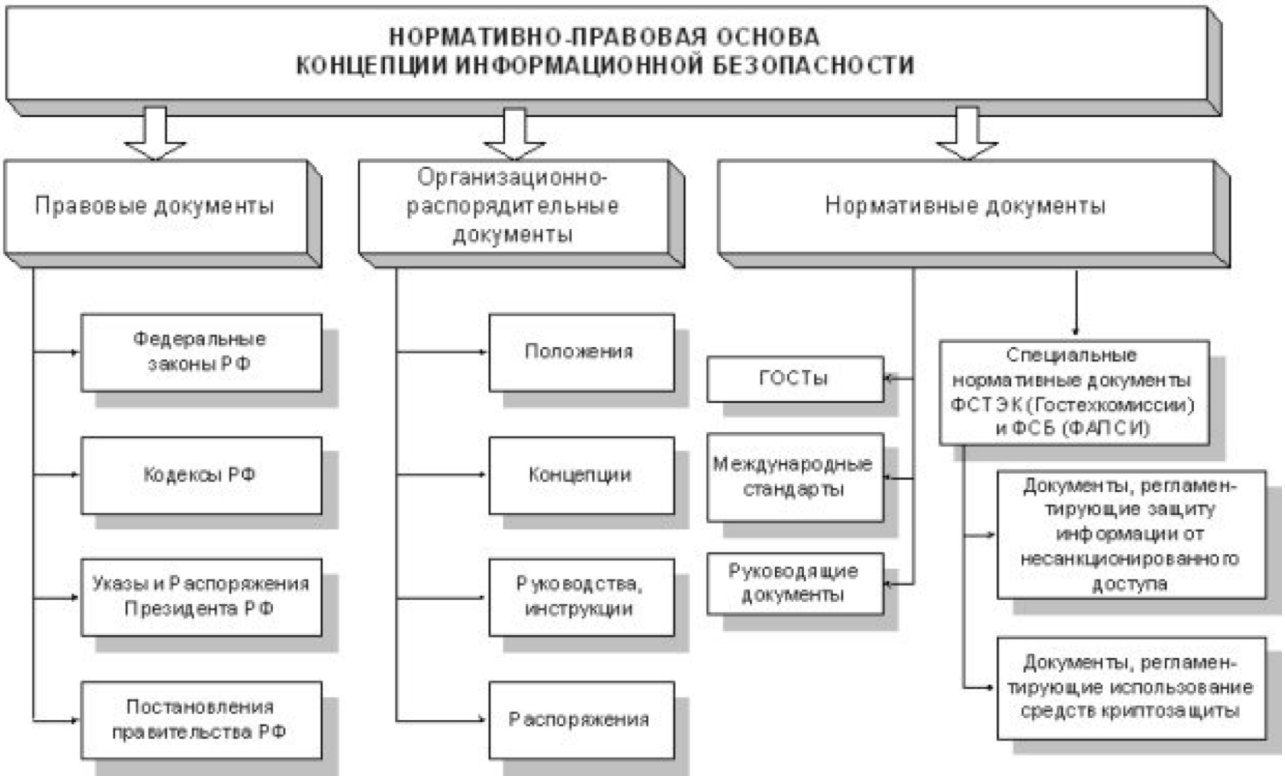
Обеспечение правовых методов ЗИ

Правовые

- Организационные
- Технически
- Программные
- Физические
- Комплексные
- Правовые

- Нормотворческая деятельность:
  - Создание законодательства в области информационной безопасности
- Исполнительная и правоприменительная деятельность:
  - Контроль за исполнением законодательства государственными органами, организациями и гражданами;
  - Разработка процедур применения законодательства к субъектам, совершившим преступления и проступки при работе с закрытой информацией;
  - Разработка составов правонарушений с учётом специфики уголовной, гражданской, административной и дисциплинированной ответственности.

Нормативно-правовая база РФ в сфере обеспечения ИБ



ФСТЭК – Федеральная Служба по Техническому и Экспортному Контролю

Критерии безопасности компьютерных систем

- Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»);
- Европейские критерии безопасности информационных технологий;
- Руководящие документы Гостехкомиссия (ныне ФСТЭК) России;
- Федеральные критерии безопасности информационных технологий;
- «Канадские критерии»;
- Единые критерии безопасности информационных технологий.

Анализ стандартов информационной безопасности

Главная задача стандартов информационной безопасности – согласовать позиции и цели производителей, потребителей и аналитиков-классификаторов в процессе создания и эксплуатации продуктов информационных технологий.

В качестве обобщённых показателей, характеризующих стандарты информационной безопасности и имеющих значение для всех трёх сторон, выбраны следующие:

- **Универсальность**
  «Оранжевая книга» предназначалась для военных целей, её адаптация для распределённых систем и баз данных потребовала дополнительных инструментов. Т.е. она не универсальна.
  В европейских критериях были распределённые системы, коммуникационные и сетевые системы, базы данных, но также явно оговаривалась архитектура и назначение систем, к которым он может быть применён, и никак не регламентируется среда.
  Российские – имеют ограниченную сферу применения «персональные и многопользовательские системы», причём ориентация системы на обслуживание конечных пользователей является обязательным условием.
  Федеральные критерии – достаточно универсальны, в качестве объекта применения любые системы, различия проводятся только между характеристиками среды их эксплуатации.
  «Канадские критерии» – любые типы компьютерных систем.
  В единых критериях предложена технология создания ИТ продуктов, при которых использование стандарта является неотъемлемым компонентом;
- **Гибкость**
  Требования «Оранжевой книги» были слишком абстрактны и потребовали дополнений.
  Европейские критерии предусматривают специальные уровни и требования, рассчитанные на *типовые* системы.
  Документы Гостехкомиссии подробно регламентируют реализацию защиты, что снижает удобство их использования.
  В федеральных критериях впервые предложен механизм профилей защиты, с помощью которых создаются специальные наборы требований, соответствующие запросам потребителей конкретного продукта и угрозам среды эксплуатации.
  «Канадские критерии» – профиль защиты необязательный элемент и присутствует специфика при рассмотрении основных понятий безопасности, поэтому они не всегда применимы.
  Единые критерии обладают практически совершенной гибкостью, посколько позволяют пользователям выразить требования с помощью механизма профилей в форме инвариантной (не зависящей от) к механизмам реализации. Производители имеют возможность продемонстрировать с помощью проекта защиты как эти требования преобразуются на практике;
- **Гарантированность**
  «Оранжевая книга» – обязательное применение формальных методов верификации только при создании систем высшего класса защищенности.
  В европейских критериях появилось требование адекватности, которое регламентирует технологию, инструментарий, а также контроль за процессом проектирования и разработки.
  В документах Гостехкомиссии этот вопрос обошли стороной – ну вот так.
  Федеральные критерии – требования к технологии разработки и требования к процессу квалифицированного анализа.
  «Канадские критерии» – есть раздел требований к адекватности, который по объему как требования к функциональности.
  Единые критерии рассматривают гарантированность реализации защиты, как самый главный компонент информационной безопасности: многоэтапный контроль на каждой стадии разработки ИТ продукта;
- **Реализуемость**
  Плохие показатели реализуемости говорят о неприменимости стандарта.
  У всех перечисленных достаточная или высокая степень реализуемости. Единые критерии сильно круче всех остальных. Документы Гостехкомиссии не хуже других.
  Функциональных требований в единых 135 штук.

- **Актуальность**

  «Оранжевая книга» – ориентирована на продиводействие угрозам конфиденциальности.
  Европейские критерии рассматривают угрозу конфиденциальности, но больше ориентированы на целостность.
  У Гостехкомиссии единственная цель – несанкционированный доступ к информации.
  Федеральные – рассматривают все типы угроз достаточно подробно.
  «Канадские критерии» – рассматривают типовой набор угроз.
  Единые критерии – если потребители требуют внести защиту, то вносим, если нет – то нет.

Основные нормативно-правовые акты и методические документы в области защиты информации

1. Доктрина информационной безопасности РФ, утверждённая Президентом РФ 9 сентября 2000 г. № Пр-1895.
2. Обновление доктрины – Утверждена Указом Президента РФ от 5 декабря 2016 г. №646
3. Стратегия развития информационного общества в РФ, утверждённая президентом РФ 7.02.2008 № ПР-212.
4. Стратегий национальной безопасности РФ до 2020 г, утверждённая указом президента РФ от 12 мая 2009 г. №537.

Основные общие нормативные правовые акты

1. Конституция Российской Федерации.
2. Федеральный закон Российской федерации от 28 декабря 2010г № 380 – ФЗ «О безопасности»
3. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите и информации»
4. Федеральный закон от 4 мая 2011 г. №99-ФЗ « О лицензировании отдельных видов деятельности»
5. «Положение о государственной системе защиты информации РФ от иностранных технологических разведок и от её утечки по технически каналам», утверждено постановлением Совета министров – правительства РФ от 15.09.1993 № 912-51.

По вопросам защиты информации ограниченного доступа, не содержащей сведения государственной тайны(конфиденциальность информации, доступ к которой ограничен федеральными законами)

1. Указ президента РФ от 6 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
2. Постановлене Правительства РФ от 3 ноября 1994г № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»
3. *Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждён приказом Гостехкомиссиии России от 30 августа 2002г № 282.
4. Указ Президента Российской Федерации от 17.03.2008 № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
5. Приказ Федеральной службы охраны Российской Федерации от 7.08.2009 № 487 "Об утверждении положения о сегменте информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.
6. Приказ ФСТЭК России от 12 июля 2012 г. № 84 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации».
7. Приказ ФСТЭК России от 12 июля 2012 г. № 83 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации».
8. Приказ ФСТЭК России от 20 июля 2012 г. № 89 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по

исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации».

9. Приказ ФСТЭК России от 20 июля 2012 г. № 90 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации».

Руководящие документы (проверить какие актуальны)

- ГОСТ 34.003-90 Автоматизированные системы (актуализирован 06.04.2015)
- ГОСТ Р 50739-95. Средства вычислительной техники. Защиты от НСД к информации. Общие технические требования. (актуализирован 01.08.2006)
- ГОСТ Р 50922-96. Защита информации. Объект информатизаии. Факторы, воздействующие на информаци. Общие положения. (заменён ГОСТ Р 50922-2006)
- ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения (заменён ГОСТ Р 51275-2006)
- ГОСТ Р 51583-2000. Порядок создания автоматизированных систем в защищенном исполнении. (заменён в 2014 и актуализирован 06.04.2015)
- ГОСТ Р 50934-96. Защита Информации. Организация и содержание работ по защите информации об образцах военной техники от технических разведок. (актуализирован 01.08.2006)
- Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации.
- Классификация автоматизированных систем и требования по защите информации.
- ГОСТ Р ИСО/МЭК 15408-2002 Информационная технология. – Методы и средства обеспечения безопасности. – Критерии оценки безопасности информационных технологий. – Части 1, 2, 3. (заменён ГОСТ Р ИСО/МЭК 15408-1-2008)
  - ➡Руководящий документ – Безопасность информационных технология - Критерии оценки безопасности информационных технология – Часть 1: Введение и общая модель, Гостехкомисиия России, 2002.