



# Реализация основных положений Доктрины информационной безопасности

## Определения (п. 2 Доктрины)

Информационная безопасность – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Информационная инфраструктура – совокупность объектов информатизации, информационных систем и сетей связи, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров.



## Участники (п.33 Доктрины):

- собственники объектов критической информационной инфраструктуры,
- СМИ,
- организации различных сфер финансового рынка,
- операторы связи и информационных систем,
- разработчики средств и провайдеры услуг информационной безопасности,
- организации, осуществляющие образовательную деятельность в сфере информационной безопасности,
- общественные объединения, уполномоченные законодательством (АДЭ в соответствии с Распоряжением Правительства Российской Федерации от 19 января 2000г. №77-р).



## Цели (п.25, 29 Доктрины):

- поддержка инновационного и ускоренного развития систем обеспечения информационной безопасности,
- повышение конкурентоспособности российских компаний,
- защита суверенитета Российской Федерации в информационном пространстве посредством осуществления самостоятельной и независимой политики, направленной на реализацию национальных интересов в информационной сфере.

# Мероприятия по обеспечению безопасности информационной инфраструктуры зачастую не имеют комплексной основы (п.18



## Доктрины):

- структура системы обеспечения информационной безопасности должна определяться функциональностью защищаемого объекта,
- безопасность отраслей вместо отрасли безопасности,
- обеспечение безопасности начинается с полного недоверия и завершается формированием доверенной среды (разработки и функционирования),
- единство нормативного правового регулирования, технического регулирования (стандартизации) и образовательно-просветительской деятельности.

# Международное сотрудничество в сфере стандартизации

Преимущества:

-образовательные,

-имиджевые, возможность отстаивать национальные  
интересы,

-участие в международном разделении труда.

Риски:

-отсутствие стратегии или последовательных и  
профессиональных действий по ее реализации приводят к  
принятию международных документов, не соответствующих  
национальным интересам.

# Обеспечение целостности, устойчивости и безопасности функционирования ЕСЭ Российской Федерации (п.8, п.23 Доктрины):



- от сети связи общего пользования - к сервисной инфраструктуре общего пользования,
- мониторинг, оповещение, управление (координация),
- управление качеством,
- подтверждение соответствия установленным требованиям.



# Осуществление оперативно-разыскных мер (п.2 Доктрины):

- СОРМ как средство обеспечения информационной безопасности,
- совершенствование нормативной правовой базы,
- обеспечение совместимости оборудования,
- совершенствование стендового оборудования для тестирования СОРМ (имитатор ПУ).



# Развитие национальной системы управления российским сегментом сети

## Интернет (п.29, 36 Доктрины):

- Интернет – это IP-протокол, который объединяет для совместной работы сети, пользовательские устройства, информационные ресурсы,
- российский сегмент сети Интернет - неотъемлемая составная часть ССОП,
- повышение роли, технической оснащённости и ответственности координационного центра национального домена сети Интернет,
- повышение эффективности взаимодействия в рамках КЦ государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности.



# Повышение эффективности профилактики правонарушений, совершаемых с использованием ИКТ (п.23 Доктрины):



-мониторинг, анализ и расследование угроз (инцидентов, уязвимостей) информационной безопасности,

-принятие организационных, процедурных, технологических и правовых мер по созданию доказательной базы совершения правонарушений.



# Развитие кадрового потенциала (п.27 Доктрины):

- использование возможностей базовых кафедр в университетах,
- открытие учебно-исследовательских центров мониторинга, анализа и расследования инцидентов информационной безопасности,
- совершенствование преподавания информатики и ИКТ в школах,
- обеспечение защищенности граждан от информационных угроз за счет формирования культуры личной информационной безопасности.



# Базовые подходы

- Рассмотрение совместно с обеспечением безопасности вопросов обеспечения доверия
- Изучение вопросов безопасности применительно к защищаемому объекту
- Взаимосвязь трех основных компонентов обеспечения информационной безопасности:
  - нормативного правового регулирования,
  - технического регулирования,
  - просветительской и культурологической деятельности.

# Нормативное правовое регулирование





# Нормативное правовое регулирование (продолжение)

- Конституция Российской Федерации
- Доктрина информационной безопасности Российской Федерации
- ФЗ «Об информации, информационных технологиях и защите информации»
- ФЗ «О техническом регулировании»
- ФЗ «О персональных данных»
- ФЗ «О связи»
- ФЗ «Об электронной подписи»
- Закон РФ «О государственной тайне»
- ФЗ «Об оперативно-разыскной деятельности»
- Отдельные Указы Президента РФ, Постановления Правительства Российской Федерации, приказы министерств, ведомств и пр.

# Техническое регулирование



- Данное направление тесно связано с деятельностью секции по развитию стандартизации и добровольной сертификации НТС Россвязи, а также с деятельностью системы добровольного подтверждения соответствия «Связь-Эффективность», образованной АДЭ совместно с Россвязью
- Применение стандартов безопасности, обеспечивает общность и эффективность решений по сравнению с использованием уникальных подходов
- Использование общих профилей безопасности обеспечивает совместимость и повторяемость решений, уменьшает стоимость и время внедрения
- Стандарты стимулируют тестирование и использование новых технологий и бизнес-моделей



# Разработка, производство и эксплуатация средств обеспечения информационной безопасности

*Примеры фундаментальных технологий:*

архитектура безопасности, управление безопасностью, безопасность взаимодействия (кибербезопасность), управление доступом и идентификацией, объектная идентификация, ИОК и защищенные директории, обнаружение вторжений, противодействие фроду, противодействие вредоносному ПО, криптография, телебиометрия...

*Примеры приложений:*

IoT, IIoT, Cloud computing, E-payment, E-commerce, E-health, SDN, NFV, M2M, IPv6, ITS, NFC, Smart Grid, Big Data...

*Примеры организационно-процедурных методов:*

Страхование, доверенная среда, уровень зрелости, общие критерии, подтверждение соответствия установленным требованиям

# Просветительские (гуманитарные) аспекты обеспечения ИБ



- Формирование культуры информационной безопасности
- Этика в сфере использования ИКТ
- Обеспечение баланса интересов личности, общества и государства в информационной сфере
- Профилактика правонарушений, совершаемых с использованием ИКТ
- Проведение молодёжных форумов по вопросам формирования культуры информационной безопасности