

Кибербезопасность критической информационной инфраструктуры в свете новой Доктрины ИБ РФ

Николай Домуховский
Директор ДСИ
ООО «УЦСБ»

О чем речь?

Доктрина ([лат. *doctrina*](#) — «учение, наука, обучение, образованность»^[1]) — [философская](#), [политическая](#) либо правовая [теория](#), [религиозная концепция](#), [учение](#), система [воззрений](#), руководящий теоретический или политический [принцип](#).

Wikipedia

Информационная безопасность Российской Федерации – состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства

Доктрина ИБ РФ - 2000

информационная безопасность Российской Федерации – 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

Доктрина ИБ РФ - 2016

Формирование доктрины



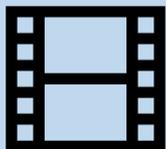
Формирование доктрины



Общая степень зрелости ИБ



Геополитическая ситуация



Оснащенность кадрами

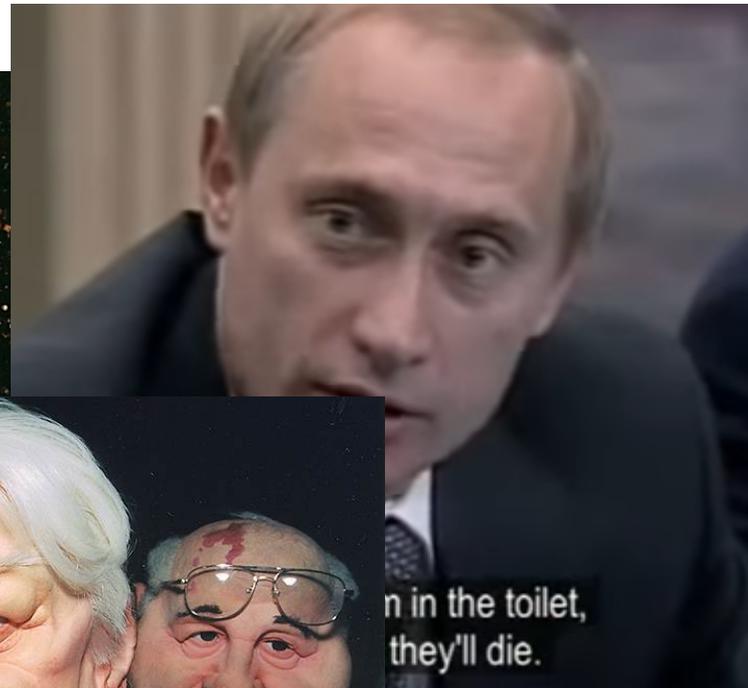


Экономика



Нормативная база

Что было в 2000-м?



n in the toilet,
they'll die.

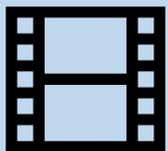
WORLD TRADE
ORGANIZATION



Что было в 2000-м?



- «Старый» трехглавый закон, закон о государственной тайне
- Закон о государственной тайне
- Система сертификации СрЗИ, аттестации ОИ
- Криминализация компьютерных преступлений



- Появление «гражданской» специальности по защите информации
- «утечка мозгов»



- Активное вступление в мировое сообщество (ВТО и пр.)
- Ориентация на международные стандарты
- Ориентация на экспорт собственной высокотехнологичной продукции
- Вторая чеченская война



- «Переваривание» результатов приватизации
- Живы последствия августа 1998



- Отставание по информационно-телекоммуникационным технологиям
- Отставание по нормативно-правовому регулированию
- Отставание по кадровой подготовке
- Понимание, что надо развиваться во всех направлениях

Доктрина-2000

ИБ – защита национальных интересов РФ

**соблюдение прав и свобод
на доступ к информации и
пользование ею**

**Информационное
обеспечение внешней и
внутренней политики РФ**

Развитие ИТК-систем

**Защита информационных
ресурсов от НСД**

- Электронное правительство и ГИС
- Обеспечение конституционных прав граждан (поиск, распространение информации, личная тайна)
- Интеллектуальная собственность
- Развитие СМИ
- Персональные данные

Доктрина-2000

ИБ – защита национальных интересов РФ

соблюдение прав и свобод
на доступ к информации и
пользование ею

Информационное
обеспечение внешней и
внутренней политики РФ

- Укрепление государственных СМИ
- Доступ на зарубежный рынок СМИ
- Развитие ГИС

Развитие ИТК-систем

Защита информационных
ресурсов от НСД

Доктрина-2000

ИБ – защита национальных интересов РФ

соблюдение прав и свобод
на доступ к информации и
пользование ею

Информационное
обеспечение внешней и
внутренней политики РФ

Развитие ИТК-систем

Защита информационных
ресурсов от НСД

- Развитие инфраструктуры единого информационного пространства РФ
- Развитие индустрии информационных услуг
- Развитие отечественного производства и выход на международный рынок
- Государственная поддержка исследований в сфере коммуникации, ИТ и ИБ

Доктрина-2000

ИБ – защита национальных интересов РФ

соблюдение прав и свобод
на доступ к информации и
пользование ею

Информационное
обеспечение внешней и
внутренней политики РФ

Развитие ИТК-систем

Защита информационных
ресурсов от НСД

- Повысить безопасность *объектов защиты*
- Развитие рынка отечественных СрЗИ
- Защита гостайны
- Развитие международного сотрудничества

Доктрина-2000. Объекты защиты

повысить безопасность информационных систем, включая

- сети связи, прежде всего безопасность первичных сетей связи
- и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации,
- финансово - кредитной и банковской сфер,
- сферы хозяйственной деятельности, а также
- систем и средств информатизации вооружения и военной техники,
- ~~систем управления войсками и оружием,~~
- [систем управления] экологически опасными и экономически важными производствами;

Доктрина ИБ РФ 2000 г. (по мотивам)



Доктрина-2000. Источники угроз



Доктрина-2000. А что там с АСУ ТП?

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как:

...

разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;

Наиболее уязвимыми объектами обеспечения информационной безопасности Российской Федерации в условиях чрезвычайных ситуаций являются система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении чрезвычайных ситуаций

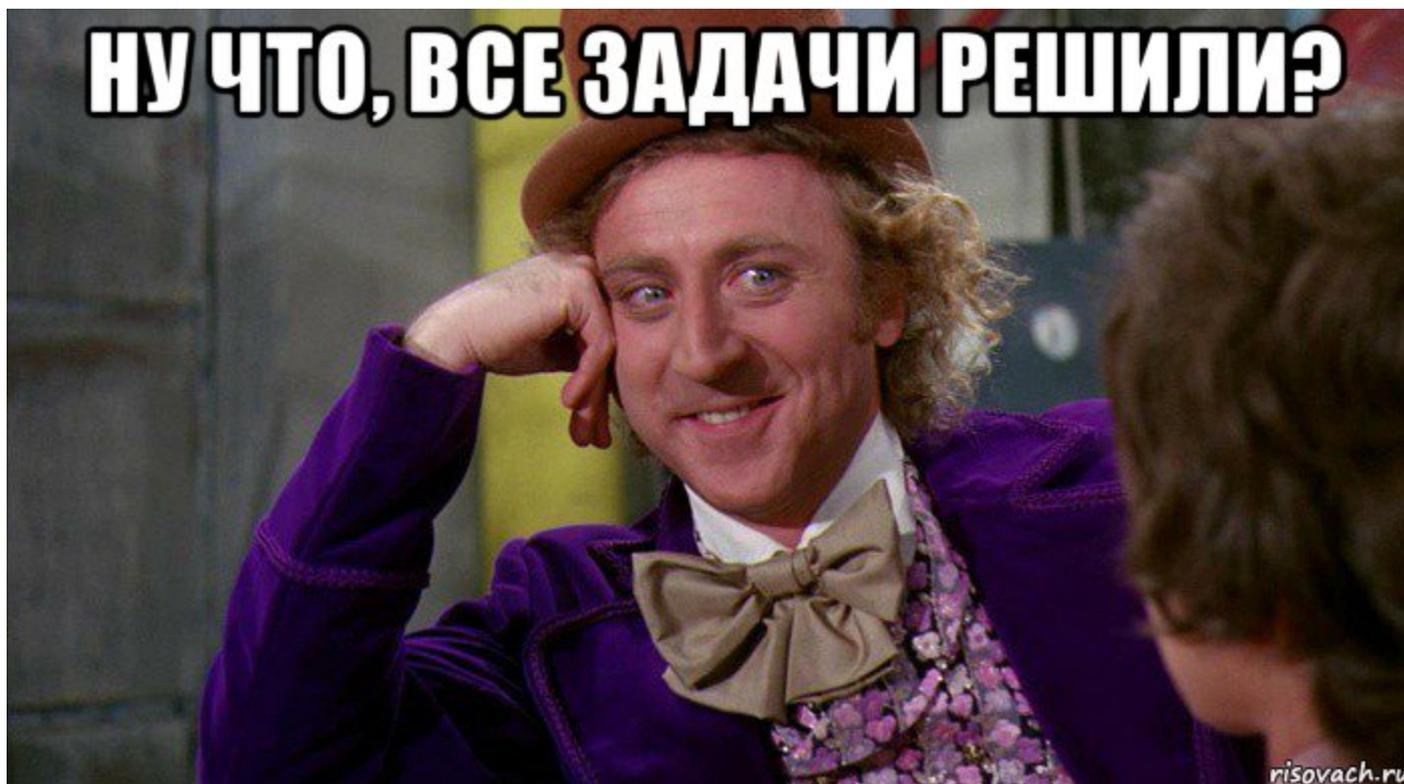
...

К специфическим для данных условий направлениям обеспечения информационной безопасности относятся:

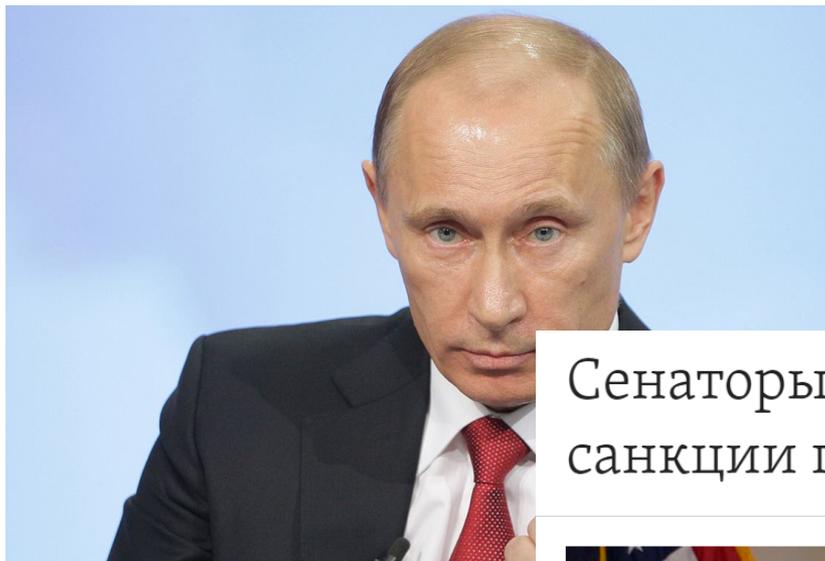
...

разработка специальных мер по защите информационных систем, обеспечивающих управление экологически опасными и экономически важными производствами.

Доктрина-2000. А что там с АСУ ТП?



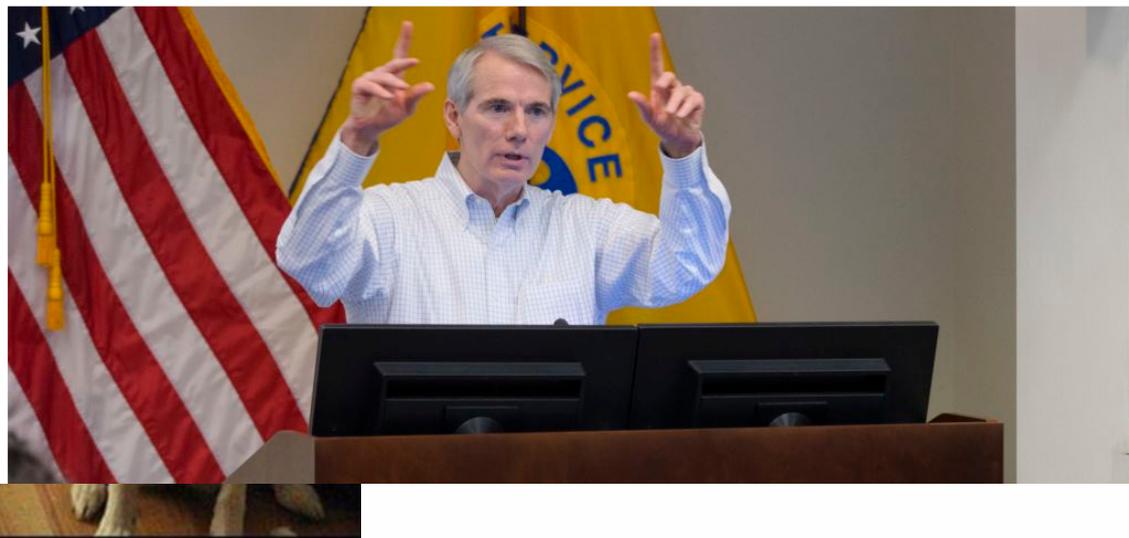
А что у нас в 2016-м?



Сенаторы призывают Трампа ужесточить санкции против России



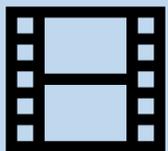
THE
RUSSIANS
DID IT!



А что у нас в 2016-м?



- Устоявшиеся правила на рынке ИБ
- ПДн, коммерческая тайна, развитое отраслевое регулирование
- Новый «трехглавый» закон
- Антитеррористические законы



- Развитие специальностей в области ИБ
- Все равно кадровый голод



- Курс на изоляцию
- Санкции
- «Импортозамещение»
- ИБ в «популярной» международной повестке

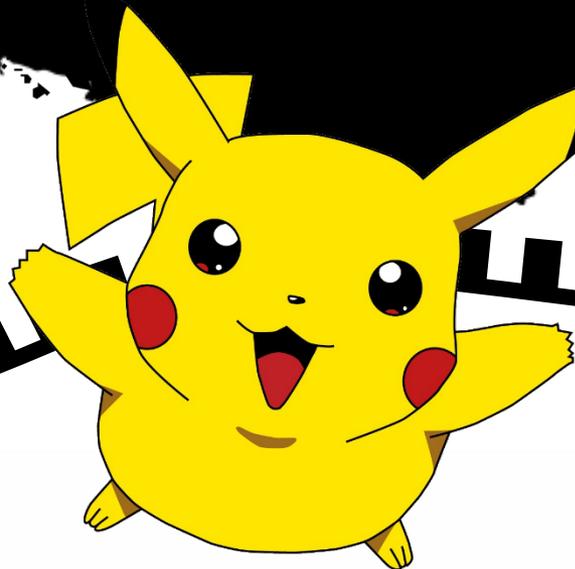


- Пока еще есть запасы от «тучных» лет
- Развитие экономических связей с азиатскими странами



- Появление явных приоритетов: теперь только защита от угроз

Доктрина-2016



Доктрина-2016

Информационная безопасность Российской Федерации – состояние *защищенности* ее национальных *интересов в информационной сфере*, определяющихся совокупностью сбалансированных интересов личности, общества и государства

Доктрина ИБ РФ - 2000

информационная безопасность Российской Федерации – 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

Доктрина ИБ РФ - 2016

Доктрина-2016. А что там с АСУ ТП?

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

...

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;

Участниками системы обеспечения информационной безопасности являются: **собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты**, ... организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности

Доктрина-2016. Чего ждать?

- Принятие закона «О безопасности критической информационной инфраструктуры Российской Федерации»
- Активизация работ по реализации плана основных направлений государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации
- Усиление внимания к вопросу за пределами профессиональной сферы
- ...
- Много работы 😊

Благодарю за внимание!

Николай Домуховский

**ООО «УЦСБ»
620100, Екатеринбург, ул. Ткачей, д.6
Тел.: +7 (343) 379-98-34
Факс: +7 (343) 382-05-63**

info@ussc.ru

www.USSC.ru