

Основы информационной безопасности РФ

Лекция 5. Система управления информационной безопасностью РФ



Задание на СР

- 1. Ответить на вопрос (к лекции №5). Какие системы включены в список ключевых систем информационной инфраструктуры таможенных органов РФ?**

Вводная часть

Лекция № 5. Система управления информационной безопасностью РФ

Тема № 2.1. Государственная политика РФ в области информационной безопасности.

Модуль №2. Нормативно-правовые основы информационной безопасности в Российской Федерации.

Цель занятия: Рассмотреть систему управления информационной безопасностью РФ.

- 1. Государственная система управления информационной безопасностью РФ.**
- 2. Иерархия нормативно-правовых актов РФ в области информационной безопасности.**
- 3. Мировая практика управления информационной безопасностью.**

Вводная часть

Литература:

А) Основная

Башлы, П.Н. Основы информационной безопасности в таможенных органах РФ: учебник/ П.Н. Башлы.– Ростов н/Д: Российская таможенная академия, Ростовский филиал, 2014.

Б) Дополнительная

Галатенко, В.А. Стандарты информационной безопасности: учебное пособие. - 2-е изд./ [Галатенко В.А., Бетелин В.Б.](#) – М.: Интуит.ру, 2012.

1

Государственная система управления информационной безопасностью РФ

1. Государственная система управления информационной

безопасностью РФ



Основным государственным органом, определяющим политику РФ в сфере информационной безопасности,

Вывод:

Государственная система управления информационной безопасностью сформирована и охватывает все уровни государственного управления.



обеспечения информационной безопасности РФ; в пределах своей компетенции

разрабатывают нормативные акты исполнительной власти субъектов Российской Федерации и принимают правовые акты в этой области

2

Иерархия нормативно- правовых актов РФ в области информационной безопасности

2. Иерархия нормативно-правовых актов РФ в области информационной безопасности

Правовые методы обеспечения информационной безопасности

Разработка

РФ

Разработка

Вывод:

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности РФ.

президента РФ, доктрины и концепции

Конституция РФ

Международные нормы и обязательства

3

Мировая практика управления информационной безопасностью

3. Мирровая практика управления информационной

В области информационных технологий, ISO (Международная Организация по Стандартизации, ИСО) и IEC (Международная Электротехническая Комиссия, МЭК) организован совместный технический комитет, **ISO/IEC (ИСО/МЭК) JTC 1**. Основной задачей совместного технического комитета является подготовка

Международных Стандартов	В области информационной
ISO27000	ISO/IEC 27000:2009 - Определения и основные принципы.
ISO27001	ISO/IEC 27001:2005/ BS 7799-2:2005 - Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.
ISO27002	ISO/IEC 27002:2005, BS 7799-1:2005 - Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.
ISO27003	ISO/IEC 27003:2010 - Руководство по внедрению системы управления информационной безопасностью.
ISO27004	ISO/IEC 27004:2009 - Измерение эффективности системы управления информационной безопасностью.
ISO27005	ГОСТ Р ИСО/МЭК 27001-2006 . Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

3. **Мировая практика управления информационной безопасностью**

ГОСТ Р ИСО/МЭК 27001-2006 - Система менеджмента ИБ

Система менеджмента информационной безопасности (СМИБ) (information security management system, ISMS) - часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

Цель построения СМИБ - выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон.

ГОСТ Р ИСО/МЭК 27001-2006 - Система менеджмента ИБ

Система управления информационной безопасностью на основе стандарта ISO 27001 позволяет:

- 1. Выявлять основные угрозы безопасности для существующих информационных (бизнес) –**
- 2. Обеспечить эффективное управление системой в критичных ситуациях.**
- 3. Облегчить интеграцию подсистемы информационной безопасности с ISO 9001:2000.**
- 4. Проводить процесс выполнения политики безопасности (находить и исправлять слабые места в системе информационной безопасности).**
- 5. Четко определить личную ответственность за информационную безопасность.**

ГОСТ Р ИСО/МЭК 27001-2006 - Система менеджмента ИБ

Система управления информационной безопасностью на основе стандарта ISO 27001 позволяет:

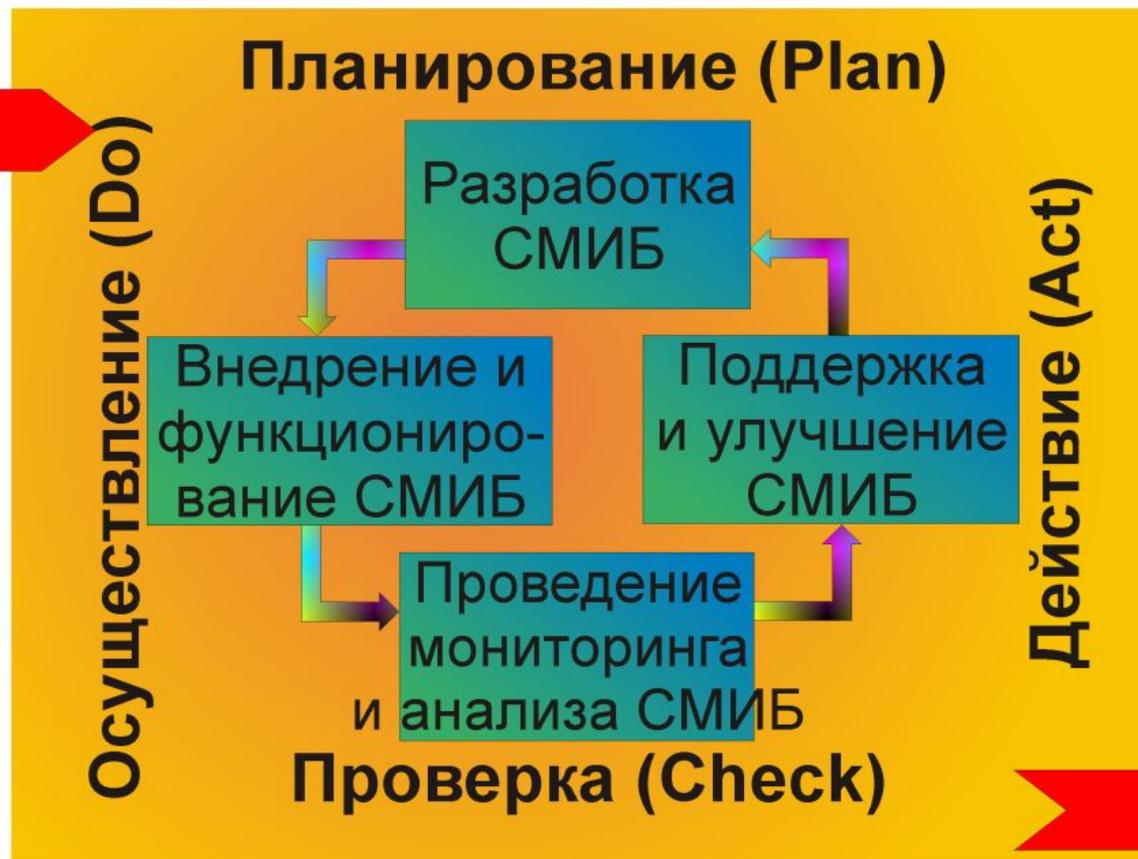
- 6. Подчеркнуть прозрачность и чистоту бизнеса перед законом благодаря соответствию стандарту.**
- 7. Продемонстрировать клиентам, партнерам, владельцам бизнеса свою приверженность к информационной безопасности.**
- 8. Получить международное признание и повышение авторитета компании, как на внутреннем рынке, так и на внешних рынках.**

ГОСТ Р ИСО/МЭК 27001-2006 - Система менеджмента ИБ

МОДЕЛЬ PDCA

Заинтересованные стороны

Требования и ожидаемые результаты в области информационной безопасности



Управляемая информационная безопасность

Заинтересованные стороны

3. **Мировая практика управления информационной**

ГОСТ Р ИСО/МЭК 27001-2006 - Система менеджмента ИБ

Планирование (разработка СМИБ)

Разработка политики, установление целей, процессов и процедур СМИБ, относящихся к менеджменту риска и улучшению информационной безопасности, для достижения результатов, соответствующих общей политике и целям организации.

Осуществление (внедрение и обеспечение функционирования СМИБ). Внедрение и применение политики информационной безопасности, мер управления, процессов и процедур СМИБ.

Проверка (проведение мониторинга и анализа СМИБ)

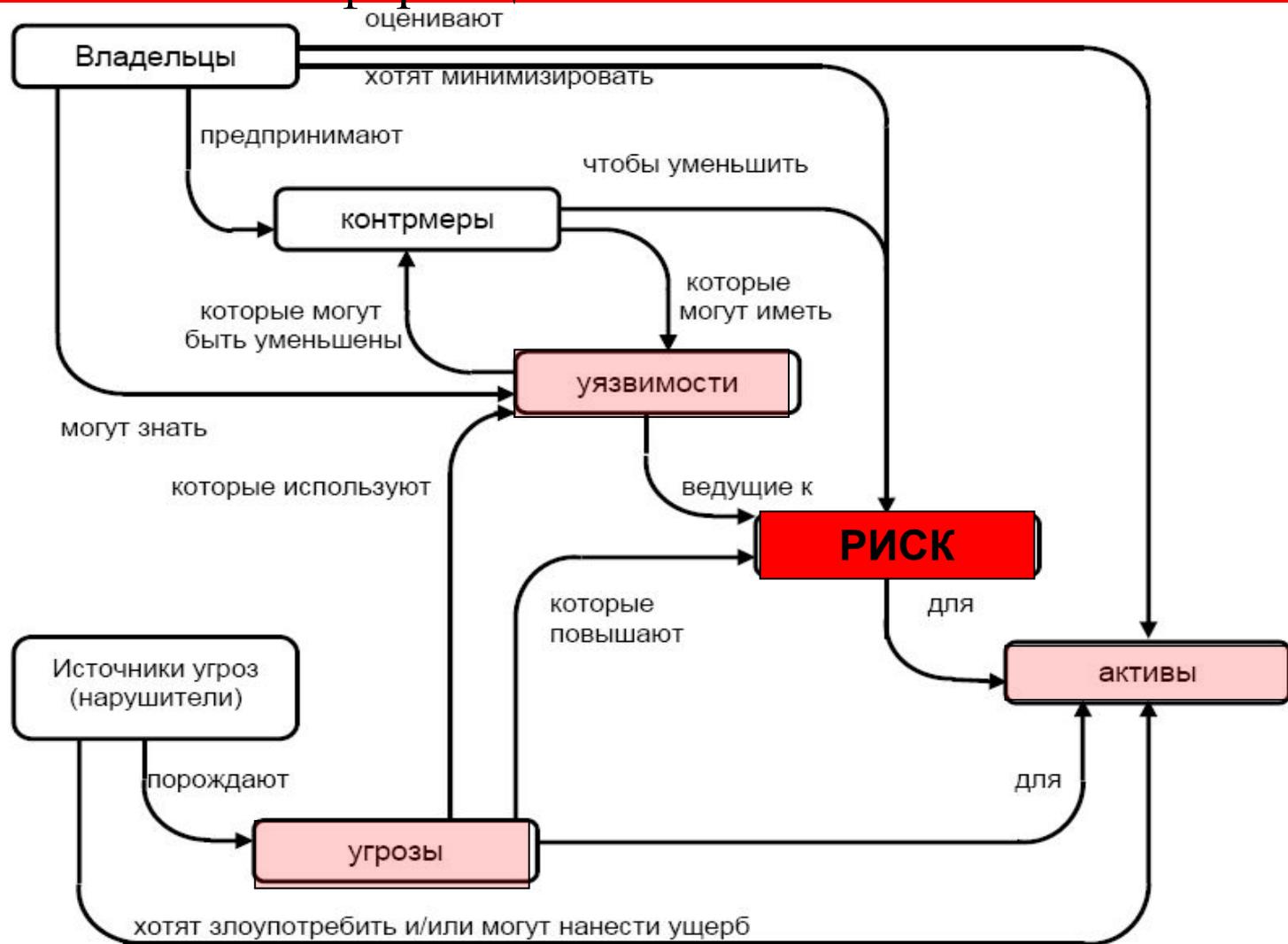
Оценка, в том числе, по возможности, количественная, результативности процессов относительно требований политики, целей безопасности и практического опыта функционирования СМИБ и информирование высшего руководства о результатах для

Действие (поддержка и улучшение СМИБ)

Проведение корректирующих и превентивных действий, основанных на результатах внутреннего аудита или другой соответствующей информации, и анализа со стороны руководства в целях достижения непрерывного улучшения СМИБ.

3. Мировая практика управления информационной

ГОСТ ИСО/МЭК 15408-2008 «Критерии оценки безопасности информационных технологий»



Модель построения системы защиты информации

ГОСТ ИСО/МЭК 15408-2008 «Критерии оценки безопасности информационных технологий»

Активы (asset) - все, что имеет ценность и подлежит защите.

Контрмеры - действия, процедуры и механизмы, обеспечивающие

Риск (risk, сочетание вероятности события и его последствий) -
потенциальная возможность нанесения ущерба в результате реализации некоторой угрозы с

ИСПОЛЬЗОВАНИЕМ УЯЗВИМОСТЕЙ АКТИВОВ.

Угрозы (threat) - совокупность условий и факторов, создающих потенциальную или реально существующую возможность нарушения информационной безопасности.

Задание на СР

- 1. Ответить на вопрос (к 17.11.2015 г.). Что скрывается за аббревиатурой РКІ? Основные элементы РКІ?**