Основы информационной безопасности РФ

Лекция 4. Государственная политика РФ в области информационной безопасности

Задание на СР

1. **Ответить на вопрос (к лекции №4).** Наиболее эффективные и часто реализуемые методы социальной инженерии для нарушения информационной безопасности?

Вводная часть

Лекция № 4. Государственная политика РФ в области информационной безопасности.

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

Модуль №1. Нормативно-правовые основы информационной безопасности в Российской Федерации.

Цель занятия: Рассмотреть государственную систему информационной безопасности РФ.

1. **Политика РФ в области информационной безопасности.**
2. **Сравнительная характеристика государственной политики РФ и США в области информационной безопасности.**
3. **Критически важные объекты и ключевые системы информационной инфраструктуры.**

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

Политика РФ в области информационной безопасности

Основы государственной политики РФ

Государственная политика РФ в области информационной безопасности отражает отношение государства к проблеме информационной безопасности, определяет содержание деятельности органов власти всех уровней, направленной на защиту интересов личности, общества и государства.

Основные принципы государственной политики обеспечения информационной безопасности **(Доктрина ИБ)**

1. **Соблюдение Конституции РФ**, законодательства РФ, общепризнанных принципов и норм международного права **при осуществлении деятельности по обеспечению информационной безопасности РФ**.

2. **Открытость в реализации функций органов власти** всех уровней и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ.

1. Политика РФ в области информационной безопасности

Основные принципы государственной политики обеспечения информационной безопасности **(Доктрина ИБ)**

3. **Правовое равенство всех участников процесса и**

Вывод:

Государственная политика РФ базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

2

Сравнительная характеристика государственной политики РФ и США в области информационной безопасности

2. Сравнительная характеристика государственных политик РФ и США в области информационной безопасности

Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ (Доктрина ИБ)	Государственные приоритеты США по обеспечению информационной безопасно-сти (**Национальная стратегия достиже-ния безопасности в киберпространстве**» («National Strategy to Secure Cyberspace»))
Разработка и внедрение механизмов реализации правовых норм, регулирую-щих отношения в информационной сфере, осуществление государственной информационной политики.	**Становление и развитие национальной системы** реагирования на происшествия в сфере информационной безопасности.

2. Сравнительная характеристика государственных политик РФ и США в области информационной безопасности

Создание безопасных информационных технологий для ключевых систем информационной инфраструктуры крупных в

Обеспечение защиты информационных систем, имеющих отношение к

Вывод:

Государственная политика РФ в области информационной безопасности ориентируется на ведущий мировой опыт.

вопросам за

2. Сравнительная характеристика государственных политик РФ и США в области информационной безопасности

«Международная стратегия США для киберпространства». 2011 г.

Из всех угроз американской национальной безопасности руководство США больше всего опасается потенциальных масштабных атак в киберпространстве

В июле 2011 года Пентагон признал **Internet местом проведения наступательных и оборонительных операций**, как море, суша и воздух.

19.10.11 координатор госдепартамента по вопросам, относящимся к киберпространству, Кристофер Пейнтер заявил, что США оставляют за собой право использовать любые средства, в том числе и военные, для отражения кибератак.

Возможность использования для отражения кибератак не только информационных, экономических и дипломатических, **но и военн**

возможностей США.

3

Критически важные объекты и ключевые системы информационной инфраструктуры

3. Критически важные объекты и ключевые системы информационной инфраструктуры

Критически важный объект (КВО) – объект, оказывающий существенное влияние на национальную безопасность РФ, прекращение или нарушение функционирования которого приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны, либо для жизнедеятельности населения, проживающего на соответствующей территории, на длительный период времени.

Основным признаком принадлежности объекта к критически важным является наличие на объекте экологически опасного или социально значимого производства или технологического процесса, нарушение штатного режима которого приводит к ЧС определенного уровня и масштаба, а также наличие на объекте информационной системы (элементов системы), которая осуществляет функции управления чувствительными (важными) для РФ процессами

3. Критически важные объекты и ключевые системы информационной инфраструктуры

Ключевая система информационной инфраструктуры – информационно-управляющая или ИТКС, которая осуществляет управление КВО (процессом), или информационное обеспечение управления таким объектом (процессом), или официальное информирование граждан и в результате **деструктивных информационных воздействий** на которую может сложиться ЧС или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

3. Критически важные объекты и ключевые системы информационной инфраструктуры

КСИИ входят в состав:

Систем органов государственной власти.

Систем органов управления правоохранительных структур.

Систем финансово-кредитной и банковской деятельности.

Систем предупреждения и ликвидации чрезвычайных ситуаций.

Систем специального назначения.

Систем управления транспортом (наземным, воздушным, морским).

Систем управления потенциально опасными объектами и др.

Задание на СР

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