Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 1

Введение

Толстой Александр Иванович
к.т.н., доцент
Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
НИЯУ МИФИ

Москва, 2018

1. Введение

1.1. Актуальность

1.2. Структура и содержание дисциплины

1.3. Место дисциплины в учебных планах программ магистратуры

1.4. Виды контроля знаний

1.5. График проведения занятий

1.6. Рекомендуемая литература

1.1.Актуальность

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (Утверждены Президентом Российской Федерации 3 февраля 2012 г., № 803):

Критически важный объект инфраструктуры РФ (далее - КВО) - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта РФ либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок.

Пример КВО: Ядерные объекты (производство, хранение, транспортировка и переработка ядерных веществ).

Последствия чрезвычайных ситуаций: хищение опасных веществ, причинение вреда здоровью и жизни персонала объекта, населению за пределами территории объекта, катастрофическое воздействие на окружающую природную среду

1.1.Актуальность

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (Утверждены Президентом Российской Федерации 3 февраля 2012 г., № 803):

Автоматизированная система управления производственными и технологическими процессами КВО (АСУ КВО) - комплекс аппаратных и программных средств, информационных систем и информационно-телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса КВО, нарушение (или прекращение) функционирования которых может привести к тяжким последствиям.

Тяжкие последствия: нанесение вреда внешнеполитическим интересам РФ, аварии и катастрофы, массовые беспорядки, длительные остановки транспорта, производственных или технологических процессов, дезорганизация работы учреждений, предприятий или организаций, нанесение материального ущерба в крупном размере, смерть или нанесение тяжкого вреда здоровью хотя бы одного человека.

1.1.Актуальность

Рекомендации по гармонизации законодательства государств – членов Организации Договора о коллективной безопасности (ОДКБ) в сфере обеспечения безопасности критически важных объектов (Приняты Постановление Парламентской Ассамблеи ОДКБ 27.11.2014 года № 7-5):

Государства – члены ОДКБ: Российская Федерация, Республика Белорусь, Республика Казахстан, Республика Такжикистан, Кыргыская Республика, Республика Армения.

Безопасность критически важного объекта (КВО) представляет собой составную часть комплекса задач по обеспечению национальной безопасности

Критически важные объекты - объекты социальной, производственной, инженерной, транспортной, энергетической, информационно-коммуникационной и иной инфраструктуры, нарушение функционирования которых в результате акта терроризма, также других негативных воздействий, может оказать влияние на принятие органами власти решений, воспрепятствовать политической или иной общественной деятельности, спровоцировать осложнение международных отношений или войну, устрашить население, дестабилизировать общественный порядок и (или) повлечь за собой человеческие жертвы, причинение вреда здоровью людей или окружающей среде, значительный материальный ущерб и нарушение условий жизнедеятельности людей.

1.2. Структура и содержание дисциплины ОИБ КВО

Тематический план дисциплины

«Основы информационной безопасности критически важных объектов»

1.Введение

2.Базовая терминология

3. Нормативно-правовое обеспечение

4. Исходная концептуальная схема обеспечения ИБ

5. Защита информации от несанкционированного доступа

6. Защита информации от воздействий вредоносных программ

7. Криптографические методы защиты информации

8. Защита информации от утечки по техническим каналам

9. ИБ автоматизированных систем критически важных объектов

10. ИБ и системы физической защиты критически важных объектов

1.2. Структура и содержание дисциплины ОИБ КВО

Тематический план дисциплины

«Основы информационной безопасности критически важных объектов»

1.Введение

2.Базовая терминология

http://online.mephi.ru

3. Нормативно-правовое обеспечение

4. Исходная концептуальная схема обеспечения ИБ

5. Защита информации от несанкционированного доступа

6. Защита информации от воздействий вредоносных программ

7. Криптографические методы защиты информации

8. Защита информации от утечки по техническим каналам

9. ИБ автоматизированных систем критически важных объектов

10. ИБ и системы физической защиты критически важных объектов

1.3. Место дисциплины в учебных планах программ магистратуры

Учебные планы, к которым относится дисциплина «Основы информационной безопасности критически важных объектов»:

1. Направление: 14.04.01 «Ядерная энергетика и теплофизика»

1.1. Магистерская программа «Безопасное обращение с ядерными материалами». (группа М17-181)

2. Направление: 14.04.02 «Ядерные физика и технологии»

2.1.Магистерская программа «Системы автоматизации физических установок и их элементы» (группы М17-182, М17-С81)

2.2. Магистерская программа «Теплофизика ядерных энергетических установок». (группы М17-С82, М17-С83)

Структура дисциплины: лекции – 4 учебных часов (уч), практические занятия – 4 уч; самостоятельная работа – 64 уч. Всего – 72 уч

1.4. Виды контроля знаний

Текущий контроль - контроль посещения; фиксация активности во время занятий;

Итоговый контроль: зачет* (зачетная сессия)

*** - возможен в виде сдачи тестов**

1.5. График проведения занятий:

06.03.2018 с 16.00 – 19.00 (Моск.время) –Лекции: Тема 1, Тема 2

13.03.2018 по 15.05.2018 – самостоятельная работа: изучение Тем 3,…,10 на http://online.mephi.ru

08.05.2018 с 16.00 -18.00 (Моск.время) – Практические занятия: комментарий к вопросам, вынесенным на тестирование; инструктаж использования дистанционного тестирования

15.05.2018 с 16.00 -18.00 (Моск.время) – Дистанционное тестирование

1.6. Рекомендуемая литература ***(www.techbook.ru)***

Учебная литература:

1.Введение в информационную безопасность: Учебное пособие для вузов/ А.А.Малюк, В.С.Горбатов, В.И.Королев и др.; Под ред. В.С.Горбатова . – М.: Горячая линия–Телеком, 2011. – 288 с.

2.Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов . – М.: Горячая линия–Телеком, 2001. – 148 с.

3.Серия «Вопросы управление информационной безопасностью»:

3.1. Книга 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2014. – 244 с.

3.2.Книга 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2014. – 130 с.

3.3.Книга 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2014. – 139 с.

3.4.Книга 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2014. – 186 с.

3.5.Книга 5: Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2014. – 145 с.

4. Физическая защита ядерных объектов: Учебное пособие для вузов/ П.В.Бондарев, А.В.Измайлов, А.И.Толстой; Под ред. Н.С.Погожина.- М.: МИФИ, 2008.- 584 с.

1.5. Рекомендуемая литература (www.techbook.ru)

Дополнительная литература:

1. Малюк А.А. Теория защиты информации . – М.: Горячая линия–Телеком, 2012. – 184 с.
2. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере ИБ. . – М.: Горячая линия–Телеком, 2012. – 140 с.

Благодарю за внимание!

Толстой Александр Иванович
Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ)
кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем НИЯУ МИФИ

AITolstoj@mephi.ru