



Управление информационной безопасностью

Учебная дисциплина УИБ-М

Тема **1.** Введение

Толстой Александр Иванович

К.Т.Н., доцент

Доцент кафедры «Информационная безопасность банковских систем»

НИЯУ МИФИ,

Факультет «Кибернетика и информационная безопасность»,
кафедра



Москва, февраль
2016



1. Место дисциплины в учебном плане магистерских программ

Направление подготовки: 10.04.01 – «Информационная безопасность»

Квалификация: магистр

Магистерские программы:

1. «Применение методов криптологии в системах обеспечения информационной безопасности» (каф.42)
2. «Обеспечение безопасности информации ключевых систем информационной инфраструктуры» (каф.43)
3. «Обеспечение непрерывности и информационной безопасности бизнеса» (каф.44)
4. «Информационно-аналитическое обеспечение финансового мониторинга» (каф.75)

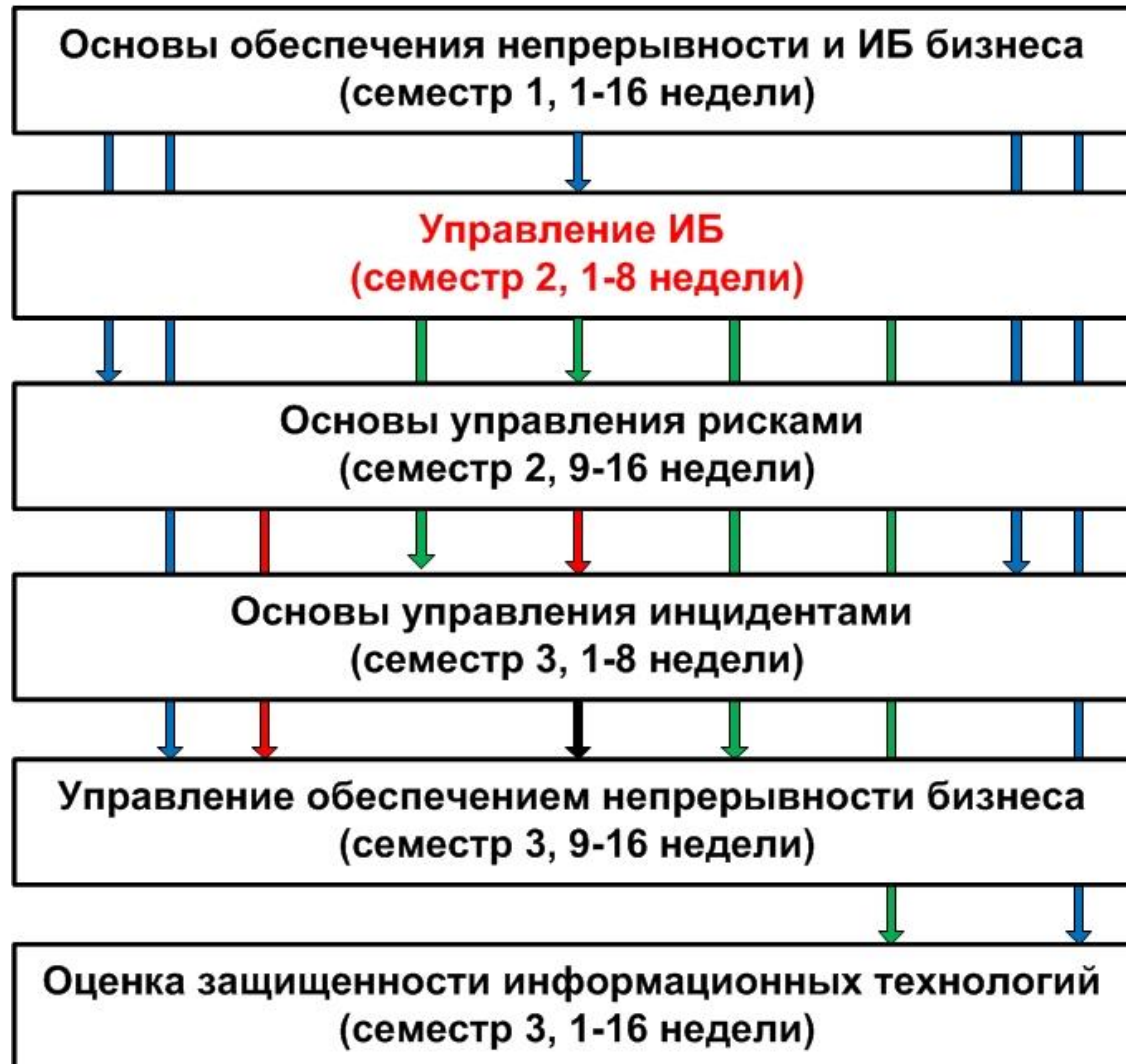
Форма обучения: очно-заочно (дистанционно)

Семестр: 2 (1-8 недели)

Структура дисциплины:

лекции – 16 учебных часов;
практические занятия (семинары) – 16
самостоятельная работа – 40
Всего 72 учебных часа

1. Место дисциплины в учебном плане магистерской программы каф.44



2. Особенности дисциплины

Задача учебной дисциплины: формирование у студентов профессиональных компетенций, необходимых для решения задач, относящихся к определенному виду профессиональной деятельности.

Объект профессиональной деятельности: система управления информационной безопасностью – СУИБ;

Вид профессиональной деятельности: «организационно-управленческая деятельность».

Задачи профессиональной деятельности:

- организация управления информационной безопасностью;

Приобретаемые профессиональные компетенции:

- способностью принимать участие в управлении информационной безопасностью
- способностью на практике применять стандарты, относящиеся к обеспечению информационной безопасности

2. Особенности дисциплины

В результате изучения дисциплины студенты должны:

“Иметь представление”:

- о современной концепции обеспечения ИБ, базирующейся на управленческом подходе;
- о принципах построения СУИБ;
- о взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ.

“Знать”:

- основные стандарты, регламентирующие управление ИБ;
- принципы разработки процессов управления ИБ;
- подходы к интеграции СУИБ в общую систему управления предприятием.

“Уметь”:

- анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ;
- определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
- применять процессный подход к управлению ИБ в различных сферах деятельности;

“Владеть”:

- терминологией и процессным подходом построения систем

Структура и содержание дисциплины:

Очное обучение:

Введение**

- 1. Концептуальные основы обеспечения ИБ***
- 2. Концептуальные подходы к управлению ИБ***
 - 2.1. Политики ИБ. Угрозы ИБ****
- 3. Концептуальные подходы к управлению рисками***
- 4. Концептуальные подходы к управлению инцидентами***
- 5. Концептуальные подходы к контролю обеспечения ИБ***

Заочное обучение:**

7. Основы управления ИБ: освоение электронного образовательного курса (ЭОК), содержащего лекционный материал:

ЭОК-1 «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ» (324 экрана)

Самостоятельная работа: выполнение домашних заданий

***- кроме гр. Б02-44М**

**** - все группы**

Структура и содержание дисциплины (ЭОК):

Тема 1. Введение

Тема 2. Современные подходы к обеспечению ИБ.

Тема 3. Процессный подход в рамках управления ИБ.

Тема 4. Документы в области ИБ.

Тема 5. Политики ИБ.

Электронный образовательный курс «Управление ИБ»

1. БАЗОВАЯ ТЕРМИНОЛОГИЯ

1.1. Понятие «информационная безопасность»

1.2. Понятие «система»

1.3. Понятие «управление»

1.4. Понятие «процесс»

2. СТАНДАРТИЗАЦИЯ СИСТЕМ И ПРОЦЕССОВ УПРАВЛЕНИЯ ИБ

2.1. Серия стандартов 27000 «Информационная технология. Методы обеспечения безопасности»

2.2. Характеристики стандартов, относящихся к управлению ИБ

2.3. Стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ

2.4. Отраслевые стандарты в области управления ИБ – стандарты Банка России

3. ПОЛИТИКА ИБ

3.1. Понятия ПолиИБ

3.2. Виды ПолиИБ

3.3. Основные требования и принципы, учитываемые при разработке и внедрении ПолиИБ

3.4. Содержание политики ИБ

3.5. Жизненный цикл политики ИБ

3.6. Ответственность за исполнение ПолиИБ

4. УПРАВЛЕНИЕ И СИСТЕМА УПРАВЛЕНИЯ ИБ

4.1. Необходимость управления ОИБ организации

4.2. Деятельность по ОИБ организации как процесс

4.3. Определение управления ИБ организации

4.4. Цель и задачи управления ИБ организации

4.5. Уровни и функциональная структура управления ИБ организации

4.6. Управление ИБ информационно-телекоммуникационных технологий организации

4.7. Система управления ИБ организации

4.8. Процессный подход в рамках управления ИБ

4.9. Работа с процессами СУИБ организации

4.10. Стратегии построения и внедрения СУИБ

1.4. Виды контроля знаний

Текущий контроль:

- контроль активности в системе дистанционного обучения
- контроль посещения;
- фиксация активности во время занятий.

Промежуточный контроль:

- контроль освоения ЭОК-1: зачет с оценкой* (8-ая неделя)
- выполнение домашних заданий с оценкой

Итоговый контроль: зачет** (17-ая неделя)

*- в виде сдачи тестов в системе дистанционного обучения

** - как средняя оценка видов промежуточного

1.5. Темы домашних заданий

Задание 1.

Разработка проекта документа «Политика ИБ объекта» (организации)»

Задание 2.

Разработка проекта документов «Модель угроз ИБ объекта» и Модель нарушителя ИБ организации» (только Б02-44М)

Выбор объекта (необходимо согласовать с преподавателем и руководителем ВКР):

Объект исследования из выпускной квалификационной работы (ВКР):

- **Организация в целом;**
- **Объект информатизации.**

1.6. Рекомендуемая литература (www.techbook.ru)

Учебная литература:

Серия «Вопросы управление информационной безопасностью»:

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.

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. 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.

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.

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.

Дополнительная литература:

1. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере ИБ. . – М.: Горячая линия–Телеком, 2012. – 140 с.

Благодарю за внимание!

Толстой Александр Иванович

AITolstoj@mephi.ru

8(499)324-97-35