Приложение №3 «Рабочие программы дисциплин» к образовательной программе по направлению подготовки 38.03.02 Менеджмент (бакалавриат)

Рабочая программа дисциплины «Информационная безопасность»

Утверждена:

Дата: 2018.

Подпись:

М.П.

1. Цели дисциплины

Формирование у студентов знаний в области защиты информации от несанкционированного доступа, умений и навыков практического обеспечения информационной безопасности.

Задачи дисциплины:

Подготовка бакалавров, обладающих знаниями, навыками, умениями в сфере обеспечения информационной безопасности организаций различных форм собственности.

2. Перечень формируемых компетенций в процессе освоения дисциплины

По окончанию освоения дисциплины обучающийся должен обладать следующими общекультурными компетенциями (ОК):

- способностью работать в коллективе, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия (ОК-5);
- способностью к самоорганизации и самообразованию (ОК-6);

общепрофессиональными компетенциями (ОПК):

- способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-7).

3. Место дисциплины в структуре ООП ВО

Дисциплина является элементом вариативной части Блока 1 образовательной программы.

4. Объем дисциплины

Показатели объема дисциплины	**Форма обучения**	
	Очная	**Заочная**
Объем дисциплины в зачетных единицах	3	3
Объем дисциплины в часах	108	108
Лекционные занятия	16	-
Лабораторные работы	-	-
Практические занятия	50	8
Самостоятельная работа студентов	38	96
Контроль	4	4

Формой текущего контроля и промежуточной аттестации являются:
- для очной формы обучения зачет в 5 семестре;
- для заочной формы обучения зачет на 4 курсе.

Очная форма обучения

№	Темы (разделы) дисциплины	Лекционные занятия	Лабораторные работы	Практические занятия
1.	Введение в информационную безопасность	2	-	6
2.	Правовое обеспечение информационной безопасности	2	-	6
3.	Организационное обеспечение информационной безопасности	2	-	4
4.	Технические средства и методы защиты информации	2	-	6
5.	Программно-аппаратные средства и методы обеспечения информационной безопасности	2	-	8
6.	Криптографические методы защиты информации	2	-	6
7.	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	2	-	8
8.	Использование криптографических средств защиты информации	2	-	6
Итого		**16**	**-**	**50**

Заочная форма обучения

№	Темы (разделы) дисциплины	Лекционные занятия	Лабораторные работы	Практические занятия
1.	Введение в информационную безопасность	-	-	1
2.	Правовое обеспечение информационной безопасности	-	-	1
3.	Организационное обеспечение информационной безопасности	-	-	1

4.	Технические средства и методы защиты информации	-	-	1
5.	Программно-аппаратные средства и методы обеспечения информационной безопасности	-	-	1
6.	Криптографические методы защиты информации	-	-	1
7.	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	-	-	1
8.	Использование криптографических средств защиты информации	-	-	1
Итого		**-**	**-**	**8**

5. Содержание программы учебной дисциплины

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)	Коды компетенций
Тема 1	**Введение в информационную безопасность**	Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации.	**ОК-5 ОК-6**
Тема 2	**Правовое обеспечение информационной безопасности**	Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.	**ОК-5 ОК-6**
Тема 3	**Организационное обеспечение информационной безопасности**	Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.	**ОК-5 ОК-6**
Тема 4	**Технические средства и методы защиты информации**	Инженерная защита объектов. Защита информации от утечки по техническим каналам	**ОК-5 ОК-6 ОПК-7**
Тема 5	**Программно-аппаратные**	Основные виды сетевых и компьютерных угроз. Средства	**ОК-5 ОК-6**

	средства и методы обеспечения информационной безопасности	и методы защиты от сетевых компьютерных угроз	**ОПК-7**
Тема 6	**Криптографические методы защиты информации**	Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы	**ОК-5** **ОК-6** **ОПК-7**
Тема 7	**Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности**	Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности	**ОК-5** **ОК-6** **ОПК-7**
Тема 8	**Использование криптографических средств защиты информации**	Создание зашифрованных файлов и криптоконтейнеров и их расшифрование	**ОК-5** **ОК-6** **ОПК-7**

6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа предполагает изучение литературных источников, использование Internet-данных, изучение нормативно-правовой базы, выполнение самостоятельных заданий, подготовку рефератов.

Контроль за выполнением самостоятельной работы ведется в ходе изучения курса преподавателем на практических занятиях, а также при проверке индивидуальных заданий и письменных работ.

Темы самостоятельной работы

1. Понятие ценной (собственной) предпринимательской информации.
2. Ценность и полезность информации.
3. Критерии ценности информационных ресурсов.
4. Правовые и экономические предпосылки выделения ценной информации. Взаимосвязь критериев ценности и необходимости обеспечения безопасности информации.
5. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов и информационных услуг.
6. Безопасность функционирования предпринимательской структуры.

7. Концепция защиты информации.
8. Понятие и цели защиты информации, формирование и эволюция понятия.
9. Обеспечивающий технологический аспект защиты информации.
10. Виды грифов и ограничительных отметок.
11. Порядок работы персонала с конфиденциальными документами.
12. Угрозы безопасности информации в процессе публикаторской, рекламной и выставочной деятельности.
13. Анализ ценности информации.
14. Действия персонала в типовых и чрезвычайных ситуациях.

Литература для самостоятельной работы обучающихся

- Аверченков В.И. Защита персональных данных в организации [Электронный ресурс] : монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 124 c. — 5-89838-382-4. — Режим доступа: http://www.iprbookshop.ru/6993.html

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература по дисциплине:

- Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

Дополнительная литература по дисциплине:

- Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 c. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), необходимых для освоения дисциплины

- Российская государственная библиотека. (http://www.rsl.ru)
- www.iprbookshop.ru

9. Перечень программного обеспечения и информационных справочных систем (при необходимости)

- Open Office (бесплатная лицензия);
- Система «Гарант-Образование».

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

В процессе преподавания дисциплины используются следующие материально-технические средства:

- компьютер;
- маркерная доска;
- экран;
- проектор;
- колонки;
- наглядные пособия на флеш-носителе.

11. Фонд оценочных средств и описание показателей и критериев оценивания освоения материала дисциплины

Описание показателей и критериев оценивания освоения материала дисциплины:

Словесное выражение	**Описание**
Зачтено	Даны правильные ответы на более чем 50% вопросов приведены примеры, показано умение связать теорию с практикой.
Незачтено	Не дан ответ на 50% вопросов отсутствуют примеры. Ответ на вопрос полностью отсутствует. Отказ от ответа.

Методические материалы, определяющие процедуры оценивания освоенного материала и сформированности компетенций:

Текущая аттестация студентов может проводиться лектором или преподавателем, ведущим занятия по дисциплине в следующих формах:

- опрос;
- тестирование;
- выполнение заданий на занятии;
- письменные домашние задания и т.д.;
- отдельно оцениваются личностные качества студента.

Конкретные формы и периодичность проведения текущей аттестации определяются преподавателем.

Типовые контрольные задания или иные материалы характеризующие формирование компетенций в процессе освоения образовательной программы:

Типовые вопросы к зачету:

1. Место информационной безопасности в обеспечении системы общественной безопасности.
2. Основные направления и задачи обеспечения информационной безопасности общества.
3. Основные компоненты информационной безопасности автоматизированных информационных систем.
4. Уровни реализации информационной безопасности.

5. Определение и классификация информационных ресурсов.
6. Основные виды угроз информационным ресурсам.
7. Особенности угроз конфиденциальной информации.
8. Причины возникновения угроз утраты или утечки конфиденциальной информации.
9. Причины возникновения каналов несанкционированного доступа к информации.
10. Виды каналов несанкционированного доступа к информации.
11. Характер действия организационных каналов несанкционированного доступа к информации.
12. Технические каналы несанкционированного доступа к информации.
13. Особенности угроз автоматизированным информационным системам.
14. Классификация удаленных атак.
15. Основные направления правовой защиты информации.
16. Содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.
17. Законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.
18. Порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.
19. Объекты защиты авторских прав.
20. Основные права автора в отношении его произведения.
21. Объекты интеллектуальной собственности, защищаемые патентным законодательством.
22. Основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).
23. Определение государственной тайны и назвать грифы секретности.
24. Сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.
25. Порядок отнесения сведений к государственной тайне и их засекречивания.
26. Последовательность условий и формы допуска должностных лиц к государственной тайне.
27. Определение коммерческой тайны и сведения, которые не могут быть ее объектом.
28. Порядок установления режима коммерческой тайны и основные права ее субъектов.
29. Основные виды служебной тайны определенные законодательством Российской Федерации.
30. Принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.
31. Основные положения концепции информационной безопасности предприятия.
32. Содержание регламента обеспечения информационной безопасности предприятия.

33. Основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.
34. Критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.
35. Содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.
36. Критерии выделения конфиденциальных документов из общего потока поступающих документов.
37. Состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.
38. Особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.
39. Состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.
40. Особенности текста конфиденциального документа.
41. Пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.
42. Возможности, трудности и направления использования электронной почты для передачи конфиденциальных документов.
43. Задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.
44. Способы и средства физического уничтожения документов, изготовленных на носителях различных типов.
45. Пути поиска документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.
46. Технологическая схема (цепочка) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.
47. Технологическая схема (цепочка) увольнения сотрудников, владеющих конфиденциальной информацией.
48. Виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции.
49. Схема каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, степень опасности каждого канала.
50. Основные элементы физической защиты территории и помещений предприятия.
51. Способы и элементы программно-технической защиты информационных ресурсов.
52. Классификация компьютерных вирусов.
53. Основные антивирусные программы.

54. Основные способы криптографического преобразования данных.