

АННОТАЦИЯ

дисциплины «Обеспечение безопасности электронного бизнеса»

Объем трудоемкости: 3 зачетные единицы (108 часов, из них – 50.2 часов аудиторной нагрузки: лекционных 18 часов, лабораторных 32 часа; 57.8 часов самостоятельной работы; 6 часов КСР)

Цель освоения дисциплины – формирование у бакалавров представления о теоретических и практических основах защиты электронного бизнеса и концептуальными подходами их реализации.

Задачи освоения дисциплины:

Задача курса состоит в получении представления о концепции информационной безопасности на основе информационных технологий и использования системного подхода для обеспечения безопасности электронного бизнеса. Существенное значение имеет изучение основных методов, протоколов и алгоритмов, реализующих защиту информации в сетях, получение навыков оценки существующих угроз информации для электронного бизнеса.

Место дисциплины (модуля) в структуре образовательной программы

В процессе подготовки и изложения курса учтены требования стандартов Министерства образования и науки РФ, принципы компетентности, предусмотренные миссией и программами КубГУ.

Способом и средством достижения образовательных целей является усвоение учебной программы при соответствующей организации аудиторных занятий и самостоятельной работы студентов.

Занятия организуются на основе фундаментальных научных разработок отечественных и зарубежных авторов, для получения эффективных социальных и экономических результатов.

Изложение учебного курса основано на принципах компетентностного подхода. Занятия по предмету курса организованы с учетом полученных студентами знаний мировоззренческих, правовых дисциплин, теории экономики.

Дисциплина « Обеспечение безопасности электронного бизнеса» предусматривает использование знаний бакалавров, полученных ими в ходе изучения следующих дисциплин:

- «Информатика»;
- «Дискретная математика»;
- «Общая теория систем»;
- «Дифференциальные уравнения»;
- «Вычислительные системы, сети и коммуникации»;
- «Защита информации»;

Требования к уровню освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций: ПК-9, ПК-27.

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1	ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления	Основные определения причин нарушения целостности информации,	Проводить анализ архитектуры предприятия на уязвимость	Методологии математического моделирования

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
		информационной безопасностью ИТ-инфраструктуры предприятия	каналов несанкционированного получения информации, каналов копирования информации		прикладных областях; Элементами структурно-функционального мышления при решении задач формализации и алгоритмизации в конкретных областях деятельности.
2	ПК-27	способность использовать лучшие практики продвижения инновационных программно-информационных продуктов и услуг	современные стандарты де-юре, де-факто в области организации безопасности электронного бизнеса	использовать современные стандарты и методики, разрабатывать регламенты для организации управления процессами жизненного цикла ИТ-инфраструктуры предприятий	методиками оценки затрат ресурсов, методов их оптимизации и распределения

**Основные разделы дисциплины:
Разделы дисциплины, изучаемые в 6 семестре**

№ разд ела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Самостоятельная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Общее понятие безопасности и система мер по её обеспечению	10	2	2		6
2	Правовые аспекты и диагностические параметры экономической безопасности	11.8	2	4		5.8
3	Экономические разведка и контрразведка	9	2	2		5
4	Экономическая безопасность предприятия и основные её критерии и показатели	17	2	6		9
5	Анализ уровня экономической безопасности предприятия(ЭБП) и основные направления её обеспечения.	12	2	6		4
6	Проблемы обеспечения безопасности предпринимательской деятельности в России.	12	2	4		6
7	Методы информационно-аналитической работы (конкурентной разведки), применяемые для определения и оценки экономических рисков компании	12	2	4		6
8	Защита компании от экономических рисков, связанных с участием компании в гражданско-правовых отношениях	10	2	2		6
9	Зарубежный опыт обеспечения безопасности предпринимательской деятельности	8	2	2		4
<i>Итого по дисциплине:</i>		101.8	18	32		51.8

Курсовые работы: *не предусмотрены*

Форма проведения аттестации по дисциплине: экзамен в конце 6 семестра.

Основная литература:*

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа : www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7

2. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — М. : Издательство Юрайт, 2018. — 220 с. — (Серия : Университеты России). — ISBN 978-5-9916-9244-1. — Режим доступа : www.biblio-online.ru/book/6946C235-8650-4A29-B75B-68E0EF829422

3. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учеб. — Электрон. дан. — Минск : "Вышэйшая школа", 2017. — 324 с. — Режим доступа: <https://e.lanbook.com/book/75150>. — Загл. с экрана.

*Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

Автор

Пономаренко Т.Н., старший преподаватель