Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Ректор
/ Н.В. Дубив /
«31» августа 2020 г.

Рабочая программа учебной дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

образовательной программы высшего образования –
программы специалитета

38.05.01 Экономическая безопасность
Специализация №1 «Экономико-правовое обеспечение экономической безопасности»

Форма обучения: очная, очно-заочная, заочная

Курган 2020

Рабочая программа дисциплины «Информационная безопасность предпринимательской деятельности» составлена в соответствии с учебным планом по программе специалитета «Экономическая безопасность» (экономико-правовое обеспечение экономической безопасности), утвержденными:
- для очной формы обучения «28» августа 2020 года
- для очно-заочной формы обучения «28» августа 2020 года
- для заочной «28» августа 2020 года

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 31 августа 2020 года, протокол № 1.

Рабочую программу составил:
ст. преподаватель А.В. Человечкова

Согласовано:

Заведующий кафедрой «БИАС»
канд. пед. наук, доцент Е.Н. Полякова

Заведующий кафедрой «Финансы и экономическая безопасность»
к.э.н., доцент Н.Я. Чепелюк

Специалист по учебно-методической работе Учебно-методического отдела Г.В. Казанкова

Начальник управления образовательной деятельности С.Н. Синицын

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр 5
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**32**	**32**
Лекции	16	16
Лабораторные работы	16	16
Самостоятельная работа, всего часов в том числе:	**76**	**76**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (изучение тем, подготовка к лабораторным работам и рубежному контролю)	58	58
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Очно-заочная форма обучения

Вид учебной работы	На всю дисциплину	Семестр 5
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**18**	**18**
Лекции	6	6
Парктические работы	12	12
Самостоятельная работа, всего часов в том числе:	**90**	**90**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (изучение тем, подготовка к лабораторным работам и рубежному контролю)	72	72
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Заочная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		10
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**6**	**6**
Лекции	2	2
Лабораторные работы	4	4
Самостоятельная работа, всего часов в том числе:	**102**	**102**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (изучение тем, подготовка к лабораторным работам)	66	66
Контрольная работа	18	18
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность предпринимательской деятельности» относится к вариативной части блока 1. Дисциплина основывается на знании следующих дисциплин: «Математика», «Информационные системы в экономике», «Моделирование информационных систем».

Для успешного освоения дисциплины «Информационная безопасность предпринимательской деятельности» студент должен:

1. знать основы алгебры, математического анализа, дискретной математики, теории вероятностей и математической статистики, информатики;
2. уметь использовать современные технические средства и информационные технологии для решения аналитических и исследовательских задач;
3. владеть навыками научного познания применительно к постановке и решению задач информационной безопасности.

Изучение дисциплины необходимо для дальнейшего изучения таких дисциплин, как: «Планирование и прогнозирование в экономике» «Сетевые технологии» «Экономическая статистика», «Информационно-правовые системы».

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины «Информационная безопасность предпринимательской деятельности» является получение студентами целостного представления о современных методах и средствах обеспечения информационной безопасности и их практического применения. На основе полученных знаний сформировать у студентов системный подход к решению проблем информационной безопасности.

Задачи изучения дисциплины продиктованы требованием формирования у студентов системного подхода к решению проблем информационной безопасности:

- освоение основных понятий и терминологии информационной безопасности;
- знакомство с угрозами, которым подвергается информация, а также классификацией этих угроз и их анализом;
- изучение организационно-административных и технических методов и средств защиты информации;
- изучение криптографических методов защиты информации;
- изучение нормативно-законодательной базы и стандартов информационной безопасности и защиты информации;
- изучение моделей информационной безопасности;
- обеспечение безопасности автоматизированных систем.

В результате освоения дисциплины должны быть сформированы следующие компетенции:

— способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности - ПК20.

В результате изучения дисциплины обучающийся должен:

знать:

– основные законы, нормативно-правовые акты, руководящие документы, регулирующие отношения в сфере информационной безопасности (для ПК-20);

уметь:

– анализировать базовые документы, регулирующие аспекты информационной безопасности (для ПК-20);

владеть:

– профессиональной терминологией в области информационной безопасности (для ПК-20);

– навыками безопасного использования технических средств в профессиональной деятельности (для ПК-20);

– методами формирования требований по защите информации (для ПК-20).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план.

Очная форма обучения

Рубеж	Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем	
			Лекции	Лаборатор. работы
Рубеж 1	Тема 1	Основные понятия и определения информационной безопасности	2	1
	Тема 2	Информационная безопасность в системе национальной безопасности РФ	2	2
	Тема 3	Нормативно законодательная база и стандарты в области информационной безопасности	2	1
	Тема 4	Угрозы информационной безопасности, их классификация и анализ	2	2
	Рубежный контроль 1		-	1
Рубеж 2	Тема 5	Общие сведения о методах и средствах обеспечения информационной безопасности	2	2
	Тема 6	Информационная безопасность автоматизированных систем	2	2
	Тема 7	Криптографические основы информационной безопасности	2	2
	Тема 8	Информационная безопасность	2	2

		компьютеров и компьютерных сетей		
	Рубежный контроль 2		-	1
		Всего:	**16**	**16**

Очно-заочная форма обучения

Рубеж	Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем	
			Лекции	Практич. работы
Рубеж 1	Тема 1	Основные понятия и определения информационной безопасности	1	-
	Тема 2	Информационная безопасность в системе национальной безопасности РФ	1	-
	Тема 3	Нормативно законодательная база и стандарты в области информационной безопасности	1	2
	Тема 4	Угрозы информационной безопасности, их классификация и анализ	-	2
	Рубежный контроль 1		-	1
Рубеж 2	Тема 5	Общие сведения о методах и средствах обеспечения информационной безопасности	1	2
	Тема 6	Информационная безопасность автоматизированных систем	-	2
	Тема 7	Криптографические основы информационной безопасности	1	2
	Тема 8	Информационная безопасность компьютеров и компьютерных сетей	1	-
	Рубежный контроль 2		-	1
		Всего:	**6**	**12**

Заочная форма обучения

Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем	
		Лекции	Лаборатор. работы
Тема 2	Информационная безопасность в системе национальной безопасности РФ	0,5	-
Тема 3	Нормативно законодательная база и стандарты в области информационной безопасности	0,5	-
Тема 4	Угрозы информационной безопасности, их классификация и анализ	0,5	2
Тема 7	Криптографические основы информационной безопасности	0,5	2
Всего:		**2**	**4**

4.2. Содержание лекционных занятий

Тема 1. Основные понятия и определения информационной безопасности.

Цели и задачи курса, общая характеристика его содержания. Основные понятия и определения: информация, категории информации, носители информации, информационный ресурс, безопасность информации, информационная безопасность, информационная война, информационное оружие, защита информации, средства защиты информации, автор и собственник информации, субъекты информационного обмена и их взаимодействие.

Тема 2. Информационная безопасность в системе национальной безопасности РФ.

Понятие национальной и информационной безопасности РФ. Основные составляющие информационной безопасности. Национальные интересы, безопасность и основные угрозы безопасности России в информационной сфере. Государственная информационная политика. Государственная тайна. Место информационной безопасности экономических систем в национальной безопасности страны.

Тема 3. Нормативно законодательная база и стандарты в области информационной безопасности.

Основные нормативно-справочные документы. Законодательная база информационной безопасности. Доктрина информационной безопасности РФ. Отечественные и зарубежные стандарты в области информационной безопасности. Руководящие документы Федеральной службы по техническому и экспортному контролю Минобороны России (Гостехкомиссии России).

Тема 4. Угрозы информационной безопасности, их классификация и анализ.

Понятие угрозы. Виды угроз. Нарушители информационной безопасности. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз. Классификация угроз по способам их негативного воздействия и на основе методов системного анализа. Классификация атак, уровни безопасности. Уязвимости и политика безопасности.

Тема 5. Общие сведения о методах и средствах обеспечения информационной безопасности.

Организационно-административные, технические, криптографические методы защиты информации. Модели каналов передачи информации. Коды обнаруживающие и исправляющие ошибки. Защита информации в автоматизированных системах обработки данных. Защита системы и данных в современных ОС. Механизмы информационной безопасности Идентификация и аутентификация, управление доступом.

Тема 6. Информационная безопасность автоматизированных систем.

Информационные системы и связанные с их функционированием угрозы. Причины нарушения целостности информации и возможные злоумышленные действия в автоматизированных системах обработки данных. Модель нарушителя информационных систем. Модели информационной безопасности и их использование. Таксономия и анализ способов нарушения информационной безопасности. Модели оценки угроз. Модели защиты информации. Методы определения требований к защите информации. Функции и стратегии защиты информации. Архитектура систем защиты информации.

Тема 7. Криптографические основы информационной безопасности.

Криптология, составляющие ее компоненты и основные этапы развития. Принципы криптографической защиты информации. Модели открытых текстов, критерии распознавания открытого текста Шифры, их классификация, теоретическая и практическая стойкость. Аппаратная и программная реализация шифров. Определение симметричных и асимметричных криптографических систем. Блочные и поточные шифры, принципы их построения. Линейные регистры сдвига и их композиции. Принципы построения криптосистем с открытым ключом. Криптосистема RSA. Российский и зарубежные стандарты шифрования.

Тема 8. Информационная безопасность компьютеров и компьютерных сетей.

Цели, функции и задачи защиты информации в компьютерах и компьютерных сетях. Информационная безопасность в условиях функционирования в России глобальных сетей. Архитектура механизмов защиты информации. Разработка защищенных приложений в средах программирования. Принципы и средства защиты электронной почты. Методы защиты межсетевого обмена данными, использование межсетевых экранов. Компьютерные вирусы и их классификация. Способы заражения программ. Методы защиты. Антивирусные программы. Программно-технические средства защиты информации в компьютере

4.3 Лабораторные работы (практические работы)

Номер раздела, темы	Наименование раздела, темы	Наименование лабораторного занятия	Количество часов контактной работы с преподавателем		
			Очная форма	Очно-заочная форма	Заочная форма
1	Основные понятия и определения информационной безопасности	Лабораторное занятие №1. Изучение основных понятий и определений информационной безопасности.	1	-	-
2	Информационная безопасность в системе национальной безопасности РФ	Лабораторное занятие №2. Изучение сравнительных характеристик систем баз данных с правовой информацией «Консультант Плюс», «Гарант» и определение лучшей из них.	2	-	-
3	Нормативно законодательная база и стандарты в области информационной безопасности	Лабораторное занятие №3. Знакомство с правовой базой в области защиты информации.	1	2	-
4	Угрозы информационной безопасности, их классификация и анализ	Лабораторное занятие №4. Изучение классифицирования угроз и атак на информационную систему.	2	2	2
	1-ый рубежный контроль	***Тестирование***	***1***	1	-
5	Общие сведения о методах и средствах обеспечения информационной безопасности	Лабораторное занятие №5. Создание и управление учетными записями пользователей средствами защищенной операционной системы Windows.	2	2	-
6	Информационная безопасность автоматизированных систем	Лабораторное занятие №6. Исследование защиты с применением пароля, а также методы противодействия атакам на пароль.	2	2	-
7	Криптографические основы информационной безопасности	Лабораторное занятие №7. Изучение основных методов криптографической защиты информации.	2	2	2
8	Информационная безопасность автоматизированных систем	Лабораторное занятие №8. Получение навыков выполнения контроля настроек и работы антивирусных средств на примере программы «Dr.Web CureIt!».	2	-	-
	2-ой рубежный контроль	***Тестирование***	***1***	1	-
		Всего	**16**	**12**	**4**

4.4 Контрольная работа для заочной формы обучения

В процессе выполнения контрольной работы у студентов формируются навыки ведения самостоятельной работы. Контрольные задания способствуют более углубленному изучению основ дисциплины и повышению теоретической и профессиональной подготовки студентов. Написание контрольной работу способствует лучшему усвоению материала.

Студент выбирает одну из предложенных преподавателем тем, самостоятельно готовит презентацию работы и выносит ее на обсуждение на занятии.

Результат выполнения контрольной работы оформляется в виде пояснительной записки, объемом 15-20 страниц, которая содержит:

- титульный лист;
- содержание;
- введение;
- основную часть отчета;
- заключение;
- список использованных источников;
- приложения.

При оформлении контрольной работы студент должен руководствоваться методическими указаниями к оформлению текстовой документации для студентов. По результатам проверки представленной студентом контрольной работы преподаватель принимает решение о допуске ее к защите или возвращает студенту на доработку в соответствии с отмеченными замечаниями.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение заданий на лабораторных занятиях. Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения заданий на лабораторных работах является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале занятия.

Для текущего контроля успеваемости по очной и очно-заочной формам обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на лабораторных занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным занятиям, к

рубежным контролям и подготовку к зачету, а также выполнение контрольной работы (для заочной формы обучения).

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.		
	Очная форма	Очно-заочная форма	Заочная форма
Самостоятельное изучение тем:	**38**	**58**	**62**
Основные понятия и определения информационной безопасности.	4	7	8
Информационная безопасность в системе национальной безопасности РФ.	4	7	7
Нормативно законодательная база и стандарты в области информационной безопасности.	4	7	7
Угрозы информационной безопасности, их классификация и анализ.	4	7	8
Общие сведения о методах и средствах обеспечения информационной безопасности.	6	7	8
Информационная безопасность автоматизированных систем.	6	8	8
Криптографические основы информационной безопасности.	6	8	8
Информационная безопасность компьютеров и компьютерных сетей.	4	7	8
Подготовка к лабораторным занятиям (по 2 часа на каждое занятие)	**16**	**10**	**4**
Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	**4**	**4**	-
Выполнение контрольной работы	-	-	**18**
Подготовка к зачету	**18**	**18**	**18**
Всего:	**76**	**90**	**102**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ (для очной, очно-заочной форм обучения).
2. Отчеты студентов по итогам выполнения заданий на лабораторных работах.
3. Банк тестовых заданий к рубежным контролям № 1, № 2 (для очной, очно-заочной форм обучения).
4. Вопросы к зачету.
5. Контрольная работа (для заочной формы обучения).

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

Очная форма обучения

№	Наименование	Содержание					
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	Распределение баллов					
		Вид учебной работы:	Посещение лекций	Выполнение заданий лабораторного занятия	Рубежный контроль №1	Рубежный контроль №2	Зачет
		Балльная оценка:	$2_б$ x 8= $16_б$	$3_б$ x 8 =$24_б$	15	15	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета	60 и менее баллов – неудовлетворительно; не зачтено; 61…73 – удовлетворительно; зачтено; 74… 90 – хорошо; 91…100 – отлично					
3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (зачету) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все задания, предусмотренные лабораторным курсом. Для получения зачета «автоматически» студенту необходимо набрать 61 балл По согласованию с преподавателем студенту могут быть добавлены дополнительные (бонусные) баллы за активность на лабораторных занятиях, активное участие в научной и методической работе, оригинальность идей при выполнении лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры.					
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных лабораторных занятий. Формы дополнительных заданий (назначаются преподавателем): - выполнение заданий пропущенного лабораторного занятия (при невозможности дополнительного проведения занятия преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 7 баллов. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.					

Очно-заочная форма обучения

№	Наименование	Содержание					
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	Распределение баллов					
		Вид учебной работы:	Посещение лекций	Выполнение заданий практического занятия	Рубежный контроль №1	Рубежный контроль №2	Зачет
		Балльная оценка:	$6_б$ х 3= $18_б$	$6_б$ х 5 =$30_б$	11	11	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета	60 и менее баллов – неудовлетворительно; не зачтено; 61…73 – удовлетворительно; зачтено; 74… 90 – хорошо; 91…100 – отлично					
3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (зачету) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все задания, предусмотренные практическим курсом. Для получения зачета «автоматически» студенту необходимо набрать 61 балл По согласованию с преподавателем студенту могут быть добавлены дополнительные (бонусные) баллы за активность на практических занятиях, активное участие в научной и методической работе, оригинальность идей при выполнении практических работ, за участие в значимых учебных и внеучебных мероприятиях кафедры.					
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных практических занятий. Формы дополнительных заданий (назначаются преподавателем): - выполнение заданий пропущенного практического занятия (при невозможности дополнительного проведения занятия преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 6 баллов. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.					

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий состоят для 1 и 2 рубежного контроля из 15 вопросов для очной формы обучения и 11 вопросов для очно-заочной формы обучения каждый. На каждое тестирование при рубежном контроле студенту отводится 1 академический часа.

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет проводится в форме ответа на вопросы. Вопросы к зачету доводятся до студентов на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа студенту отводится 1 астрономический час.

Результаты текущего контроля успеваемости и зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей и зачета

1-ый рубежный контроль

Вопрос 1. Доступ к информации, не нарушающий правила разграничения доступа, называется…

а) легальным;

б) нелегальным;

в) санкционированным;

г) вредоносным;

д) несанкционированным.

Вопрос 2. Субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на множество субъектов, имеющих доступ к данной информации

а) целостность;

б) доступность;

в) конфиденциальность;

г) своевременность.

Вопрос 3. Уязвимость информации — это:

а) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

б) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

в) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

Вопрос 4. К не преднамеренным угрозам относятся:

а) ошибки в разработке программных средств КС;

б) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями;

в) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой.

2-ой рубежный контроль

Вопрос 1. При парольной защите в качестве аутентификационного фактора субъекта выступает

а) то, что он знает;

б) то, чем он владеет;

в) то, что есть часть его самого.

Вопрос 2. Основные направления обеспечения КБ в зависимости от природы средств и методов:

а) компьютерное, криптографическое, бумажное

б) нормативное, формальное, практическое (экспериментальное)

в) нормативно-правовое, инженерно-техническое, организационное, аппаратно-программное.

Вопрос 3. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа:

а) антивирус;

б) замок;

в) брандма́уэр;

г) криптография;

д) экспертная система.

Вопрос 4. Для защиты от злоумышленников необходимо использовать:

а) системное программное обеспечение;

б) прикладное программное обеспечение;

в) антивирусные программы;

г) компьютерные игры;

д) музыку, видеофильмы.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Информационная безопасность и ее основные компоненты.
2. Административный и процедурный уровни информационной безопасности.
3. Механизмы информационной безопасности.
4. Политика информационной безопасности.
5. Обеспечение информационной безопасности и направления защиты.
6. Теория защиты информации. Основные направления.

7. Требования к системе защиты информации.

8. Основные положения доктрины информационной безопасности в области защиты информации.

9. Задачи обеспечения информационной безопасности на государственном уровне.

10. Основные положения, касающиеся государственной тайны.

11. Классификация атак, уровни безопасности.

12. Уязвимости и политика информационной безопасности.

13. Характер происхождения угроз.

14. Источники угроз. Предпосылки появления угроз.

15. Основные угрозы и способы обеспечения безопасности.

16. Классы каналов несанкционированного получения информации.

17. Причины нарушения целостности информации.

18. Методы и модели оценки уязвимости информации.

19. Общая модель воздействия на информацию.

20. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.

21. Классификация требований к средствам защиты информации.

22. Требования к защите, определяемые структурой автоматизированной системы обработки данных.

23. Стандарты в области информационной безопасности.

24. Функции и задачи защиты информации. Методы формирования функций защиты.

25. Стратегии защиты информации. Способы и средства защиты информации.

26. Основные аспекты проблемы кодирования.

27. Достоинства и недостатки аппаратной и программной реализации шифров.

28. Блочные системы шифрования.

29. Поточные системы шифрования.

30. Криптоаналитические атаки и их виды.

31. Модели и критерии распознавания открытых текстов.

32. Отечественный стандарт шифрования данных ГОСТ СССР 28147-89.

33. Понятие шифра, типы шифров их сильные и слабые стороны.

34.Принципы криптографической защиты информации. Симметричные и асимметричные криптосистемы.

35. Принципы разработки вычислительно стойких шифров.

36. Принципы построения криптосистем с открытым ключом.

37. Проблемы защиты информации в компьютерных сетях и пути их решения.

38. Проблемы идентификации и проверки подлинности.

39. Протоколы распределения ключей.

40. Требования к шифрам.

41.Управление криптографическими ключами: проблемы и методы их решения.

42. Шифры замены. Шифры перестановки.
43. Электронная цифровая подпись. Правовой и технический аспекты.
44. Отличительные особенности AES от DES.
45. Межсетевые экраны и их предназначение.
46. Вирусные атаки и защита от них.
47. Виды нарушений информационной системы.
48. Защита электронной почты и основные функции системы PGP.
49. Целостность данных и аутентификация сообщений.
50. Проблемы надежности шифров.
51. Проблемы защиты информации в глобальных компьютерных сетях.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

Основная литература:

1. Синадский Н.И. Защита информации в компьютерных сетях: учебное пособие / Н.И. Синадский. – Екатеринбург: УрГУ, 2008. – 225 с.

2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений. – М.: «Академия», 2005. – 256 с.

3. Завгородний, В. И. Комплексная защита информации в компьютерных системах: Учебное пособие для вузов / В.И. Завгородний. – М.: Логос, 2001. – 264 с.

4. Гафнер В.В. Информационная безопасность./ В.В. Гафнер – М.: Феникс. – 2010.- 336с.

5. Громов Ю.Ю., Драчев В.О., Иванова О.Г., Шахов Н.Г. Информационная безопасность и защита информации. – М: ООО «ТНТ». – 2010. – 384с.

6. Сухарев Е. Информационная безопасность. Методы шифрования. / Е.Сухарев– М.: Радиотехника. – 2011. – 208с.

7. Новоструев, А.В., Солодовников, В.М., Терентьева, А.А. Тезаурус в сфере информационной безопасности [Текст]/ А.В. Новоструев, В.М. Солодвников, А.А. Терентьева: Учебное пособие. – Курган: Изд-во Курганского гос. Ун-та, 2014. – 471 с.

Дополнительная литература:

1. Касперски, К. Техника сетевых атак. Т. 1 / Крис Касперски. – М.: Солон-Р, 2001. – 400 с.

2. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций: учебное пособие: для студентов вузов, обучающихся по специальности 510200 "Прикладная математика и информатика"/ О.Р. Лапонина; Интернет-университет

информационных технологий. – М.: Интернет-Университет информационных технологий, 2005. – 605 с.

3. Олифер, В.Г. Компьютерные сети: Принципы, технологии, протоколы : учебное пособие для студентов вузов / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М.; СПб.: Нижний Новгород: Питер, 2007. – 957, с.

4. Расторгуев С.П. Основы информационной безопасности: учебное пособие для студентов вузов. – М.: «Академия», 2009. – 192 с.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Галатенко В.А. Основы информационной безопасности: курс лекций: учебное пособие для студентов вузов. – М.: Интернет-Университет информационных технологий, 2004. – 261 с.

2. Нестеров С.А. Информационная безопасность и защита информации [Электронный ресурс]: Учебное пособие. – Электрон. дан. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с. – Режим доступа: свободный: http://window.edu.ru/ resource/462/67462/files/пособиеИБЗИ.pdf. – Загл. с экрана.

3. http://www.iso.org/ (Международные стандарты безопасности ISO).

4. http://www.groteck.ru/security_ru (Информационная безопасность).

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

При чтении лекций используются слайдовые презентации.

Программные средства обеспечения учебного процесса включают в себя: базовые (операционные системы; инструментальные средства программирования) и вспомогательные (программы презентационной графики; текстовые редакторы; графические редакторы).

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины включает в себя учебные аудитории и лаборатории, оснащенные современными компьютерами (все – в стандартной комплектации для практических занятий и самостоятельной работы), объединенными локальными вычислительными сетями с выходом в Интернет. Обучающемуся предоставляется возможность практической работы.

В соответствии с ООП дисциплина поддерживается соответствующими лицензионными программными продуктами.

При использовании электронных изданий вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

11. ДЛЯ СТУДЕНТОВ, ОБУЧАЮЩИХСЯ С ИСПОЛЬЗОВАНИЕМ ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений, обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины
«Информационная безопасность предпринимательской деятельности»

образовательной программы высшего образования –
программы специалитета

38.05.01 Экономическая безопасность
Специализации №1 «Экономико-правовое обеспечение экономической безопасности»

Трудоемкость дисциплины: 3 з.е. (108 академических часа)
Семестр: 5 (очная и очно-заочная формы обучения).
Семестр: 10 (заочная форма обучения)
Форма промежуточной аттестации: зачет
Содержание дисциплины. Основные разделы.

Информация как объект защиты. Информационная безопасность. Аппаратно-программные средства защиты информации. Критерии оценки безопасности компьютерных систем. Криптографические средства защиты информации. Защита от несанкционированного доступа. Типовые угрозы информационной безопасности. Технологии обеспечения безопасности в компьютерных сетях.