Частное образовательное учреждение высшего образования
«Институт социальных и гуманитарных знаний»

ЧОУ ВО «ИСГЗ»

Утверждаю
Первый проректор Димитриева Н.Т.

Рекомендовано УМС _____ председатель Романчук Е.С.

Одобрено решением кафедры Прикладной информатикии математики

Протокол № 10 от 25 мая 2017 г.

Зав. кафедрой _____ (подпись) / Зуев В.И. / к.ф.м.н., доцент

Разработчик _____ (подпись) / Зуев В.И. / к.ф.-м.н., доцент

Декан _____ (подпись) / Журавлёва Т.Б./

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Общий объем дисциплины по учебному плану 3 (з.е.), 108 часа

по направлению подготовки
09.03.03 Прикладная информатика
профиль Прикладная информатика в экономике

ФГОС ВО утвержден приказом МО и Н РФ от 12 марта 2015 г. № 207

Квалификация (степень) выпускника –бакалавр
Нормативный срок освоения программы –4 года
Форма обучения –очная, заочная

1. Цели и задачи дисциплины

Целью преподавания дисциплины «Информационная безопасность» является раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, понятие и виды компьютерных преступлений, а также приобретение студентами знаний по организационному обеспечению защиты информации и формирование некоторых практических навыков работы.

Задачи дисциплины – дать основы:

- информационного законодательства Российской Федерации;
- правил лицензирования и сертификации в области защиты информации;
- международного законодательства в области защиты информации;
- знаний о компьютерных преступлениях;
- построения систем организационной защиты объектов информатизации.

2. Место дисциплины в структуре ОП

Дисциплина «Информационная безопасность» входит в базовую часть образовательной программы.

3. Планируемые результаты освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- Способность использования основ правовых знаний в различных сферах деятельности (ОК-4)
- Способность использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий (ОПК-1)
- Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4)
- Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе (ПК-1)
- Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (ПК-18)
- Способность проводить оценку экономических затрат и рисков при создании информационных систем (ПК-21)

- Способность анализировать рынок программно-технических средств, информационных продуктов и услуг для создания и модификации информационных систем (ПК-22)
- Способность применять системный подход и математические методы в формализации решения прикладных задач (ПК-23)
- Способность готовить обзоры научной литературы и электронных информационно-образовательных ресурсов для профессиональной деятельности (ПК-24)

В результате освоения дисциплины студент должен:

знать:

- содержание основных понятий по правовому обеспечению информационной безопасности;
- правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;
- понятие и виды защищаемой информации, особенности государственной тайн как вида защищаемой информации;
- основы правового регулирования взаимоотношений администрации и персонала в области защиты информации;
- правила лицензирования и сертификации в области защиты информации;
- виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений;
- теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию;
- основные направления и методы организационной защиты информации в организациях с различными формами собственности.

уметь:

- отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности;
- разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;
- анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития;
- организовывать работу с персоналом, обладающим конфиденциальной информацией;
- организовывать охрану персонала, территорий, зданий, помещений и продукции организаций.

владеть:

- умением работы с нормативно-правовыми актами;
- умением разработки нормативно-методических материалов по регламентации системы организационной защиты информации;
- навыками применения различных способов методов защиты информации по каналам утечки и от несанкционированного доступа к ней;
- навыками построения формальных моделей систем защиты информации;
- организацией работ по обеспечению технической защиты информации ограниченного доступа (конфиденциальной информации) на территории Российской Федерации.

4. Содержание дисциплины

Общая трудоемкость дисциплины составляет 3 (з.е.), 108 (академ.часов), в т.ч.:

- *для очной формы обучения* на контактную работу обучающихся с преподавателем (аудиторные занятия) выделено 62 академ. часов, а на самостоятельную работу студентов – 44 академ. часа, форма промежуточного контроля – зачет с оценкой;
- *для заочной формы обучения* на контактную работу обучающихся с преподавателем (аудиторные занятия) выделено 12 академ. часов, а на самостоятельную работу студентов – 92 академ. часов, форма промежуточного контроля – зачет с оценкой**.**

Распределение часов курса по разделам, темам и видам работ

для очной формы обучения

Наименование тем/разделов	Всего	Аудиторные занятия (62 часов)				СРС (44 часов)		
		Всего	Лек.	Практ./ Сем.	КСР	Всего	Контрольная работа.	Самостоятельное изучение литературы
Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации Код компетенции: ОК-4	6	4	2	2		2	1	1
Тема 2. Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Код компетенции: ОПК-1	2					2	1	1
Тема 3. Виды угроз информационной безопасности Российской Федерации. Код компетенции: ПК-1	6	4	2	2		2	1	1
Тема 4. Источники угроз информационной безопасности. Код компетенции: ПК-18	2					2	1	1
Тема 5. Информационная безопасность и информационное противоборство Код компетенции: ОК-4	8	6	2	4		2	1	1
Тема 6. Обеспечение информационной безопасности объектов информатизационной сферы государства в условиях информационной войны. Код компетенции: ОПК-4, ПК-18	2					2	1	1
Тема 7. Общие методы обеспечения информационной безопасности Российской Федерации. Код компетенции: ПК-1	9	6	2	4		3	1	2
Тема 8. Основы комплексного обеспечения информационной безопасности. Код компетенции: ПК-21, ПК-22, ПК-23	3					3	1	2
Тема 9. Лицензионная и сертификационная деятельности в области защиты информации.	9	6	2	4		3	1	2

Код компетенции: ОК-4								
Тема 10. Правовые основы защиты информации с использованием технических средств. Код компетенции: ОК-4	9	6	2	4		3	1	2
Тема 11. Методы и средства обеспечения информационной безопасности компьютерных систем. Код компетенции: ОПК-4, ПК-18	6				4	2		2
Тема 12. Международное законодательство в области защиты информации. Код компетенции: ОПК-1, ПК-24	8	6	2	4		2		2
Тема 13. Система управления (менеджмента) информационной безопасности. Код компетенции: ОПК-1, ПК-23	2					2		2
Промежуточный контроль	Зачет с оценкой							
ВСЕГО	108	62	20	42	2	44	10	34

для заочной формы обучения

Наименование тем/разделов	Всего	Аудиторные занятия (12 часов)				СРС (92 часа)		
		Всего	Лек.	Практ./ Сем.	КСР	Всего	Контрольная работа.	Самостоятельное изучение литературы
Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации Код компетенции: ОК-4	12	6	2	4		6		6
Тема 2. Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Код компетенции: ОПК-1	6					6		6
Тема 3. Виды угроз информационной безопасности Российской Федерации. Код компетенции: ПК-1	6					6		6
Тема 4. Источники угроз информационной безопасности. Код компетенции: ПК-18	6					6		6
Тема 5. Информационная безопасность и информационное противоборство Код компетенции: ОК-4	6					6		6
Тема 6. Обеспечение информационной безопасности объектов информатизационной сферы государства в условиях информационной войны. Код компетенции: ОПК-4, ПК-18	6					6		6

Тема 7. Общие методы обеспечения информационной безопасности Российской Федерации. Код компетенции: ПК-1	14	6	2	4		8		8
Тема 8. Основы комплексного обеспечения информационной безопасности. Код компетенции: ПК-21, ПК-22, ПК-23	8					8		8
Тема 9. Лицензионная и сертификационная деятельности в области защиты информации. Код компетенции: ОК-4	8					8		8
Тема 10. Правовые основы защиты информации с использованием технических средств. Код компетенции: ОК-4	8					8		8
Тема 11. Методы и средства обеспечения информационной безопасности компьютерных систем. Код компетенции: ОПК-4, ПК-18	8					8		8
Тема 12. Международное законодательство в области защиты информации. Код компетенции: ОПК-1, ПК-24	8					8		8
Тема 13. Система управления (менеджмента) информационной безопасности. Код компетенции: ОПК-1, ПК-23	8					8		8
Промежуточный контроль	Зачет с оценкой (4)							
ВСЕГО	108	12	4	8	0	92	0	92

4.1 Содержание разделов дисциплины

№	Наименование раздела, темы дисциплины	Содержание раздела
1.	Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации	Понятие информации. Информация как основной объект информационного права. Специфические особенности и юридические свойства информации. Информационные отношения как объект правового регулирования. Понятие национальной безопасности. Виды безопасности. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.
2.	Тема 2. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.	Интересы личности, общества и государства в информационной сфере. Законодательный уровень информационной безопасности РФ: обзор правовых актов общего, административного и программно-технического назначения. Порядок совершения гражданско-правовых сделок, связанных с использо-

		ванием информации, обеспечение безопасности.
3.	Тема 3. Виды угроз информационной безопасности Российской Федерации.	Угрозы конституционным правам и свободам человека и гражданина в области духовной деятельности. Угрозы информационному обеспечению государственной политики Российской Федерации. Угрозы развитию отечественной индустрии информации. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.
4.	Тема 4. Источники угроз информационной безопасности.	Внешние и внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.
5.	Тема 5. Информационная безопасность и информационное противоборство.	Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности. Положение «О государственной системе защиты информации в российской федерации от иностранных технических. разведок и от ее утечки по техническим каналам». от 15 сентября 1993 г. № 912-51
6.	Тема 6. Обеспечение информационной безопасности объектов информатизационной сферы государства в условиях информационной войны.	Методы нарушения конфиденциальности, целостности и доступности информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Понятие государственной тайны. Допуск граждан Российской федерации к сведениям, составляющим государственную тайну. Система защиты государственной тайны. Организация и обеспечение режима секретности.
7.	Тема 7. Общие методы обеспечения информационной безопасности Российской Федерации.	Правовые, организационно-технические и экономические методы обеспечения информационной безопасности. Правовой режим защиты конфиденциальной информации. Правовой режим защиты коммерческой тайны. Правовой режим защиты государственных и муниципальных информационных систем.
8.	Тема 8. Основы комплексного обеспечения информационной безопасности.	Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
9.	Тема 9. Лицензионная и сертификационная деятельности в области защиты информации.	Лицензирование деятельности в области технической защиты конфиденциальной информации. Лицензирование деятельности, связанной с производством, распространением, обслуживание, средств криптографической защиты информации. Сертификация средств защиты информации. Разработка средства криптографической защиты информации.
10.	Тема 10. Правовые основы защиты информации с использованием технических средств.	Анализ правовых аспектов защиты информации на примере статьи 272, статьи 273 и статьи 274 Уголовного кодекса РФ
11.	Тема 11. Методы и средства обеспечения информационной без-	Компьютерная система как объект информационной безопасности. Общая характеристика методов и средств защиты информации. Организационно-правовые, техниче-

	опасности компьютерных систем	ские и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.
12.	Тема 12. Международное законодательство в области защиты информации.	Национальный институт стандартов и технологи (NIST). Британский институт стандартов (BSI). Международная организация по стандартизации (ISO).
13.	Тема 13. Система управления (менеджмента) информационной безопасности.	Системы менеджмента информационной безопасности на базе группы стандартов ISO 27000. Управление активами. Управление рисками информационной безопасности на базе стандарта ISO/IEC 27005. Средства и методы физической защиты объектов в соответствии с приложением A (annex A) стандарта ISO/IEC 27001. Организация пропускного и внутреобъектового режимов. Служба безопасности объектов. Введение в управление непрерывностью бизнеса.

5. Лабораторный практикум

Не предусмотрен

6. Практические занятия (семинары)

№ п/п	Наименование раздела (темы)	Вопросы семинаров/практических занятий	Трудоемкость (час.)	
			очная форма	заочная форма
1	Информационная безопасность в системе национальной безопасности Российской Федерации	**Семинар** 1.Понятие информации. Информация как объект информационного права. Специфические особенности и юридические свойства информации. 2.Информационные отношения как объект правового регулирования. 3. Понятие национальной безопасности. 4. Виды безопасности. Основные понятия и общеметодологические принципы теории информационной безопасности. 5. Роль информационной безопасности в обеспечении национальной безопасности государства.	2	4
2	Национальные интересы Российской Федерации в информационной сфере и их обеспечение.	**Семинар** 1.Интересы личности, общества и государства в информационной сфере. 2. Законодательный уровень информационной безопасности РФ: обзор правовых актов общего, административного и программно-технического назначения. 3. Порядок совершения гражданско-правовых сделок, связанных с использованием информации, обеспечение без-		

		опасности.		
3	Виды угроз информационной безопасности Российской Федерации.	**Семинар** 1.Угрозы конституционным правам и свободам человека и гражданина в области духовной деятельности. 2. Угрозы информационному обеспечению государственной политики Российской Федерации. 3.Угрозы развитию отечественной индустрии информации. 4.Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.	2	
4	Источники угроз информационной безопасности.	**Семинар** 1.Внешние и внутренние источники угроз. 2. Направления обеспечения информационной безопасности государства. 3. Проблемы региональной информационной безопасности.		
5	Информационная безопасность и информационное противоборство.	**Семинар** 1.Цели информационного противоборства. 2.Составные части и методы информационного противоборства. 3. Информационное оружие, его классификация и возможности. 4. Положение «О государственной системе защиты информации в российской федерации от иностранных технических. разведок и от ее утечки по техническим каналам». от 15 сентября 1993 г. № 912-51	4	
6	Обеспечение информационной безопасности объектов информатизационной сферы государства в условиях информационной войны.	**Семинар** 1.Методы нарушения конфиденциальности, целостности и доступности информации. 2. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. 3. Понятие государственной тайны. Допуск граждан Российской федерации к сведениям, составляющим государственную тайну. Система защиты государственной тайны. 4. Организация и обеспечение режима секретности.		
7	Общие методы обеспечения информационной безопасности Россий-	**Семинар** 1. Правовые, организационно-технические и экономические методы обеспе-	4	4

	ской Федерации.	чения информационной безопасности. 2. Правовой режим защиты конфиденциальной информации. 3. Правовой режим защиты коммерческой тайны. 4. Правовой режим защиты государственных и муниципальных информационных систем.		
8	Основы комплексного обеспечения информационной безопасности.	**Семинар** 1.Модели, стратегии и системы обеспечения информационной безопасности. 2. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.		
9	Лицензионная и сертификационная деятельности в области защиты информации.	**Семинар** 1.Лицензирование деятельности в области технической защиты конфиденциальной информации. 2.Лицензирование деятельности, связанной с производством, распространением, обслуживание, средств криптографической защиты информации. 3.Сертификация средств защиты информации. 4.Разработка средства криптографической защиты информации.	4	
10	Правовые основы защиты информации с использованием технических средств.	**Семинар** 1. Правовые основы защиты информации с использованием технических средств. 2. Анализ статьи 272, статьи 273 и статьи 274 Уголовного кодекса РФ		
11	Методы и средства обеспечения информационной безопасности компьютерных систем	**Семинар** 1.Компьютерная система как объект информационной безопасности. 2.Общая характеристика методов и средств защиты информации. 3.Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. 4.Программно-аппаратные средства обеспечения информационной безопасности.	4	
12	Международное законодательство в области защиты информации.	**Семинар** 1.Национальный институт стандартов и технологи (NIST). 2.Британский институт стандартов (BSI). 3. Международная организация по стандартизации (ISO).	4	
13	Система управления (менеджмента) информационной без-	**Семинар** 1. Системы менеджмента информационной безопасности на базе группы стан-		

	опасности.	дартов ISO 27000. Управление активами. 2. Управление рисками информационной безопасности на базе стандарта ISO/IEC 27005. 3. Средства и методы физической защиты объектов в соответствии с приложением А (annex A) стандарта ISO/IEC 27001. 4. Организация пропускного и внутреобъектового режимов. Служба безопасности объектов. Введение в управление непрерывностью бизнеса.		

7. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине:

Список литературы для самостоятельного изучения приведен в разделе 9. Учебно-методическое и информационное обеспечение дисциплины.

Методические пособия:

1. Абросимов А.Г. Методические рекомендации к выполнению самостоятельной работы для студентов, обучающихся по направлению подготовки 09.03.03 «Прикладная информатика». Методическое пособие / Абросимов А.Г., Порсев А.А., Зуев В.И. – Казань: 2017. [Электронный ресурс]. – URL: http://isgz.ru/sveden/education/#docs

8. Оценочные средства для проведения текущей и промежуточной аттестации

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	**Тема 1.** Информационная безопасность в системе национальной безопасности Российской Федерации	ОК-4	Промежуточный контроль
2.	**Тема 2.** Национальные интересы Российской Федерации в информационной сфере и их обеспечение.	ОПК-1	Промежуточный контроль
3.	**Тема 3.** Виды угроз информационной безопасности Российской Федерации.	ПК-1	Промежуточный контроль
4.	**Тема 4.** Источники угроз информационной безопасности.	ПК-18	Промежуточный контроль
5.	**Тема 5**. Информационная безопасность и информационное противоборство	ОК-4	Промежуточный контроль
6.	**Тема 6.** Обеспечение информационной безопасности объектов информатизационной сферы государства в условиях информационной войны.	ОПК-4, ПК-18	Промежуточный контроль
7.	**Тема 7.** Общие методы обеспечения информационной безопасности Российской Федерации.	ПК-1	Промежуточный контроль
8.	**Тема 8.** Основы комплексного обеспечения информационной безопасности.	ПК-21, ПК-22, ПК-23	Промежуточный контроль

9.	**Тема 9.** Лицензионная и сертификационная деятельности в области защиты информации.	ОК-4	Промежуточный контроль
10.	**Тема 10.** Правовые основы защиты информации с использованием технических средств.	ОК-4	Промежуточный контроль
11.	**Тема 11.** Методы и средства обеспечения информационной безопасности компьютерных систем.	ОПК-4, ПК-18	Промежуточный контроль
12.	**Тема 12.** Международное законодательство в области защиты информации.	ОПК-1, ПК-24	Промежуточный контроль
13.	**Тема 13.** Система управления (менеджмента) информационной безопасности.	ОПК-1, ПК-23	Промежуточный контроль – зачет

Методические материалы, определяющие процедуры оценивания формирования компетенций представлены в «Фонд оценочных знаний по дисциплине Теория систем и системный анализ»

9. Учебно-методическое и информационное обеспечение дисциплины:

Основная литература

1. Лапина, М.А. Информационное право : учебное пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин ; под ред. И.Ш. Килясханова. - Москва : Юнити-Дана, 2015. - 336 с. - (Высшее профессиональное образование: Юриспруденция). - Библиогр. в кн. - ISBN 5-238-00798-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=118624
2. Ефремов, И.В. Информационные технологии в сфере безопасности: практикум : учебное пособие / И.В. Ефремов, В.А. Солопова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». - Оренбург : ОГУ, 2013. - 116 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=259178
3. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331
4. Информационная безопасность / под ред. О. Рытенкова - М. : ГРОТЕК, 2013. - № 2. - 63 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=210608
5. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. : ил. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428820
6. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стереотип. - Москва : Флинта, 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245

Дополнительная литература

7. Информационная безопасность и защита информации : сборник студенческих работ / отв. ред. А.Ю. Колябин. - М. : Студенческая наука, 2012. - 1322 с. : ил.,табл., схем. - (Вузовская наука в помощь студенту). - ISBN 978-5-00046-137-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=227774
8. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб.пособие/В.Ф. Шаньгин. – М.: ФОРУМ : ИНФРА-М, 2012. – 416 с.
9. Галатенко, В.А. Основы информационной безопасности: учеб.пособие/В.А. Галатенко. – 4-е изд. – М.: Бином, 2010. – 205 с.
10. Смирнов, А.А. Обеспечение информационной безопасности в условиях виртуализации общества.Опыт Европейского Союза: монография/А.А.Смирнов. – М.: ЮНИТИ, 2012. – 159 с.

10. Перечень ресурсов сети Интернет

1. Информационная безопасность. Защита информации - http://all-ib.ru/
2. Информационная безопасность - http://www.itsec.ru/main.php
3. Информационная безопасность - http://www.infoguard.ru/
4. Каталог решений по информационной безопасности - http://www.ru-ib.ru/
5. Информационная безопасность. Безопасник - http://bezopasnik.org/article/1.htm
6. НПО «Эшелон». Комплексная безопасность. - http://www.npo-echelon.ru/
7. Информационная безопасность. - http://info-ispdn.ru/

11. Материально-техническое обеспечение дисциплины:

Класс, оборудованный средствами оргтехники

12. Методические указания для обучающихся по освоению дисциплины

Перед началом изучения дисциплины студентам необходимо ознакомиться с содержанием рабочей программы дисциплины, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине и самостоятельной работе, имеющимся на образовательном портале института (www.isgz.ru).

Студенты осваивают знания по данной дисциплине на лекциях, практических (семинарских) занятиях и во время самостоятельной подготовки.

На лекциях обучающиеся получают основы теоретических знаний курса. Чтобы данный метод обучения был эффективным, рекомендуется:

- посещать все лекционные и практические занятия, поскольку весь тематический материал взаимосвязан между собой и теоретического овладения пропущенного недостаточно для качественного усвоения знаний по дисциплине;
- конспектировать все рассматриваемые на лекциях и практических занятиях вопросы, обратив особое внимание на его основные положения и понятия, выводы;
- перед очередной лекцией просмотреть по конспекту материал предыдущей лекции;
- выполнять все домашние задания, получаемые на лекциях или практических занятиях;
- обозначить, что в предложенном материале не совсем понятно и вызывает вопросы, чтобы найти ответ в рекомендуемой литературе или обратиться к преподавателю во время консультации или занятия;
- проявлять активность на интерактивных лекциях и семинарских занятиях, а также при подготовке к ним. Необходимо помнить, что конечный результат овладения содержанием дисциплины необходим, в первую очередь, самому студенту;
- в случаях пропуска занятий по каким-либо причинам, необходимо обязательно самостоятельно изучать соответствующий материал.

Практические занятия призваны закрепить и углубить теоретический материал, отработать навыки решения задач и системного анализа ситуаций. При подготовке к практическим занятиям студентам рекомендуется:

- определить объем теоретического материала, который необходимо усвоить;
- изучить лекционные материалы и познакомиться с рекомендуемой преподавателем литературой;
- рассмотреть различные точки зрения по изучаемой теме, используя все доступные источники информации;
- выделить проблемные области и неоднозначные подходы к решению поставленных вопросов;
- сформулировать собственную точку зрения;
- письменно выполнить практическое задание.

Самостоятельная работа обучающихся регламентируется «Методическими рекомендациями по организации самостоятельной работы студентов» (утверждено ректором ЧОУ ВО «ИСГЗ»).

Целью самостоятельной работы студентов является:

- закрепление, расширение и углубление теоретических знаний, полученных студентами на аудиторных занятиях;
- формирование умений и навыков эффективной самостоятельной профессиональной деятельности;
- приобретение опыта творческой, исследовательской деятельности;
- воспитание у студентов самостоятельности, организованности, творческой активности, потребности развития познавательных способностей.

Самостоятельная работа включает следующие виды деятельности:

- проработку лекционного материала;
- изучение программного материала, не изложенного на лекциях;
- подготовку к семинарам, практическим занятиям;
- подготовку докладов, статей, эссе;
- выполнение учебных заданий кафедр (графические работы, рефераты);
- выполнение курсовых работ и проектов;
- и др.

Перед каждым занятием студент изучает план занятия с перечнем тем и вопросов, списком литературы и домашним заданием по вынесенному на занятие материалу.

Более подробно организация самостоятельной работы студентов прописана в Методических рекомендациях по организации самостоятельной работы студентов и в методических рекомендациях по изучению конкретной дисциплины (представлены на образовательном портале института www.isgz.ru).

Частное образовательное учреждение высшего образования
«Институт социальных и гуманитарных знаний»
ЧОУ ВО «ИСГЗ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ТЕКУЩЕГО И ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ОБУЧАЮЩИХСЯ
К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Общий объем дисциплины по учебному плану 3 (з.е.), 108 часа

по направлению подготовки
09.03.03 Прикладная информатика
направленность Прикладная информатика в экономике

ФГОС ВО утвержден приказом МО и Н РФ от 12 марта 2015 г. № 207

Квалификация (степень) выпускника – бакалавр
Нормативный срок освоения программы – 4 года
Форма обучения – очная, заочная

1. Этапы формирования компетенций в процессе изучения дисциплины

Компетенции	Форма контроля	Форма компетентностно-ориентированного задания	Показатели и критерии оценивания	Шкала оценивания (баллы)
ОК-4, ОПК-1, ОПК-4, ПК-1, ПК-18, ПК-21, ПК-22, ПК-23, ПК-24	Текущий контроль (60 баллов)	Тест	Тест – 10 вопросов. Правильный ответ на 1 вопрос равен 6 баллам.	60
ОК-4, ОПК-1, ОПК-4, ПК-1, ПК-18, ПК-21, ПК-22, ПК-23, ПК-24	Промежуточный контроль (40 баллов)	Зачет	Показывает хорошие знания изученного учебного материала, самостоятельно, логично и последовательно излагает и интерпретирует материалы учебного курса. Полностью раскрывает смысл предлагаемого вопроса. Владеет основными терминами и понятиями изученного курса. Показывает умение переложить теоретические знания на предполагаемый практический опыт	40
	ИТОГО по результатам освоения дисциплины (за один семестр)			100

Критерии оценки уровней сформированности компетенций

Уровни сформированности компетенций		
пороговый (удовлетворительно)	продвинутый (хорошо)	высокий (отлично)
Баллы		
60-79	80-90	91-100

2. Оценочные средства текущего контроля (60 баллов)

Контрольно-измерительные материалы, необходимые для оценки знаний, умений, навыков и приобретенного опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины.

Тестирование

В течение курса предусмотрено проведение тестирования в виде решения тестовых заданий. На подготовку к тестированию отводится по два часа на каждую тему. Тестовое задание на каждую тему формируется преподавателем и состоит из двух вариантов по 10 вопросов в каждом варианте.

В современном образовании тестирование используется в качестве наиболее эффективной формы контроля и самоконтроля полученных знаний по соответствующим темам учебного курса. Тестирование способствует формированию профессионального мышле-

ния, повышению понятийной культуры, развитию когнитивных способностей бакалавров. Предлагаемые задания предназначены для усвоения основных положений курса, для закрепления знаний, полученных в процессе лекционного курса и самостоятельной работы с основной и дополнительной литературой.

В условиях заочной формы получения высшего образования, тестирование оказывает существенную помощь преподавателю для организации итогового контроля знаний студентов. Тестирование позволяет реально оценить знания по курсу и выявить имеющиеся пробелы в усвоении учебного материала.

Тестирование имеет ряд несомненных достоинств. Во-первых, данная форма контроля, как правило, дает достаточно надежный результат, поскольку опрос проводится по большому числу вопросов и «элемент угадывания» не имеет существенного значения. Во-вторых, все тестируемые находятся в равных условиях, а механизм проверки заданий практически исключает «предвзятость» проверяющего. Все это делает данную форму контроля убедительной не только для преподавателя, но и для самих студентов.

Результаты тестирования разбираются на практическом занятии, проводится анализ ошибок, обсуждение итогов в форме дискуссии.

При выполнении тестов необходимо обратиться к учебникам и учебным пособиям, имеющимся в библиотеке учебного заведения.

Пояснительная записка по методике оценивания контрольной работы:

Показатели и критерии оценивания контрольной работы	Шкала оценивания контрольной работы
Тестирование: 10 вопросов 1 правильный ответ равен 6 баллам	60 баллов

Примерные тестовые вопросы:

1. Кто является основным ответственным за определение уровня классификации информации?

A. Руководитель среднего звена
B. Высшее руководство
C. Владелец
D. Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

A. Сотрудники
B. Хакеры
C. Атакующие
D. Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

C. Улучшить контроль над безопасностью этой информации

D. Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

B. Необходимый уровень доступности, целостности и конфиденциальности

C. Оценить уровень риска и отменить контрмеры

D. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

A. Владельцы данных

B. Пользователи

C. Администраторы

D. Руководство

6. Что такое процедура?

A. Правила использования программного и аппаратного обеспечения в компании

B. Пошаговая инструкция по выполнению задачи

C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

D. Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

A. Поддержка высшего руководства

B. Эффективные защитные меры и методы их внедрения

C. Актуальные и адекватные политики и процедуры безопасности

D. Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

B. Когда риски не могут быть приняты во внимание по политическим соображениям

C. Когда необходимые защитные меры слишком сложны

D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?

A. Пошаговые инструкции по выполнению задач безопасности

B. Общие руководящие требования по достижению определенного уровня безопасности

C. Широкие, высокоуровневые заявления руководства

D. Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

A. Анализ рисков

B. Анализ затрат / выгоды

C. Результаты ALE

D. Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE?

A. Количественно оценить уровень безопасности среды

B. Оценить возможные потери для каждой контрмеры

C. Количественно оценить затраты / выгоды

D. Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это:

A. Среднесрочное планирование

B. Долгосрочное планирование

C. Ежедневное планирование

D. Планирование на 6 месяцев

13. Что является определением воздействия (exposure) на безопасность?

A. Нечто, приводящее к ущербу от угрозы

B. Любая потенциальная опасность для информации или систем

C. Любой недостаток или отсутствие информационной безопасности

D. Потенциальные потери от угрозы

14. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов

B. Контрмер и защитных механизмов

C. Физической безопасности и технических средств защиты

D. Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

A. Внедрение управления механизмами безопасности

B. Классификацию данных после внедрения механизмов безопасности

C. Уровень доверия, обеспечиваемый механизмом безопасности

D. Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

A. Только военные имеют настоящую безопасность

B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности

C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше

D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?

A. Угрозы х Риски х Ценность актива

B. (Угрозы х Ценность актива х Уязвимости) х Риски

C. SLE х Частоту = ALE

D. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

18. Что из перечисленного не является целью проведения анализа рисков?

A. Делегирование полномочий

B. Количественная оценка воздействия потенциальных угроз

C. Выявление рисков

D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

A. Поддержка

B. Выполнение анализа рисков

C. Определение цели и границ

D. Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

A. Чтобы убедиться, что проводится справедливая оценка

B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Что является наилучшим описанием количественного анализа рисков?

A. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности

B. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков

C. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков

D. Метод, основанный на суждениях и интуиции

22. Почему количественный анализ рисков в чистом виде не достижим?

A. Он достижим и используется

B. Он присваивает уровни критичности. Их сложно перевести в денежный вид.

C. Это связано с точностью количественных элементов

D. Количественные измерения должны применяться к качественным элементам

23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

A. Много информации нужно собрать и ввести в программу

B. Руководство должно одобрить создание группы

C. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки

D. Множество людей должно одобрить данные

24. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

A. Стандарты

B. Должный процесс (Due process)

C. Должная забота (Due care)

D. Снижение обязательств

25. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

A. Список стандартов, процедур и политик для разработки программы безопасности

B. Текущая версия ISO 17799

C. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях

D. Открытый стандарт, определяющий цели контроля

26. Из каких четырех доменов состоит CobiT?

A. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

B. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

C. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка

D. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

27. Что представляет собой стандарт ISO/IEC 27799?

A. Стандарт по защите персональных данных о здоровье

B. Новая версия BS 17799

C. Определения для новой серии ISO 27000

D. Новая версия NIST 800-60

28. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

A. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам

B. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень

C. COSO учитывает корпоративную культуру и разработку политик

D. COSO – это система отказоустойчивости

29. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

A. NIST и OCTAVE являются корпоративными

B. NIST и OCTAVE ориентирован на ИТ

C. AS/NZS ориентирован на ИТ

D. NIST и AS/NZS являются корпоративными

30. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

A. Анализ связующего дерева

B. AS/NZS

C. NIST

D. Анализ сбоев и дефектов

31. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

A. Безопасная OECD

B. ISO\IEC

C. OECD

D. CPTED

32. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

33. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

34. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

35. Защита информации от утечки это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию до-

ступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

36. Защита информации это:
1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

37. Естественные угрозы безопасности информации вызваны:
1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

38. Икусственные угрозы безопасности информации вызваны:
1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

39. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

40. К посторонним лицам нарушителям информационной безопасности относится:
1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;

5. сотрудники службы безопасности.
6. представители конкурирующих организаций.
7. лица, нарушившие пропускной режим;

41. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

42. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

43. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

44. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

45. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

46. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

47. Активный перехват информации это перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

48. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

49. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

50. Перехват, который осуществляется путем использования оптической техники называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

51. К внутренним нарушителям информационной безопасности относится:

1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

3. Оценочные средства промежуточного контроля (40 баллов)

Форма промежуточного контроля определяется учебным планом по данной дисциплине.

Зачет с оценкой

Билет состоит из двух вопросов, на которые нужно дать развернутый ответ.

Пояснительная записка по методике оценивания зачета:

Показатели и критерии оценивания зачета	Шкала оценивания зачета
Показывает хорошие знания изученного учебного материала, самостоятельно, логично и последовательно излагает и интерпретирует материалы учебного курса	10

Полностью раскрывает смысл предлагаемого вопроса	10
Владеет основными терминами и понятиями изученного курса	10
Показывает умение переложить теоретические знания на предполагаемый практический опыт	10
Итого	40

Примерный перечень вопросов:

1. Перечислите составляющие информационной безопасности.
2. Приведите определение доступности информации.
3. Приведите определение целостности информации.
4. Приведите определение конфиденциальности информации.
5. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
6. Перечислите задачи информационной безопасности общества.
7. Перечислите уровни формирования режима информационной безопасности.
8. Дайте краткую характеристику законодательно-правового уровня.
9. Какие подуровни включает программно-технический уровень?
10. Что включает административный уровень?
11. В чем особенность морально-этического подуровня?
12. Перечислите основополагающие документы по информационной безопасности.
13. Понятие государственной тайны.
14. Что понимается под средствами защиты государственной тайны?
15. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
16. Какие категории государственных информационных ресурсов определены в Законе «Об информации, информатизации и защите информации»?
17. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
18. Какие виды требований включает стандарт ISO/IEC 15408?
19. Чем отличаются функциональные требования от требований доверия?
20. В чем заключается иерархический принцип «класс – семейство – компонент – элемент»?
21. Какова цель требований по отказоустойчивости информационных систем?
22. Сколько классов функциональных требований?
23. Дайте характеристику составляющих «информационной безопасности» применительно к вычислительным сетям.
24. Перечислите основные механизмы безопасности.
25. Какие механизмы безопасности используются для обеспечения конфиденциальности трафика?
26. Какие механизмы безопасности используются для обеспечения «неотказуемости» системы?
27. Что понимается под администрированием средств безопасности?
28. Какие виды избыточности могут использоваться в вычислительных сетях?
29. Сколько классов защищенности СВТ от НСД к информации устанавливает РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?
30. Дайте характеристику уровням защиты СВТ от НСД к информации по РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?
31. Классы защищенности АС от НСД по РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации».
32. Какие классы защищенных АС от НСД должны обеспечивать идентификацию, проверку подлинности и контроль доступа субъектов в систему?
33. Показатели защищенности межсетевых экранов.

34. Классы защищенности межсетевых экранов.
35. Цели и задачи административного уровня обеспечения информационной безопасности.
36. Содержание административного уровня.
37. Дайте определение политики безопасности.
38. Направления разработки политики безопасности.
39. Перечислите составные элементы автоматизированных систем.
40. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.
41. Перечислите классы угроз информационной безопасности.
42. Назовите причины и источники случайных воздействий на информационные системы.
43. Дайте характеристику преднамеренным угрозам.
44. Перечислите каналы несанкционированного доступа.
45. В чем особенность «упреждающей» защиты в информационных системах.
46. Характерные черты компьютерных вирусов.
47. Дайте определение программного вируса.
48. Какие трудности возникают при определении компьютерного вируса?
49. Когда появился первый вирус, который самостоятельно дописывал себя в файлы?
50. В чем особенность компьютерного вируса «Чернобыль»?
51. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
52. Перечислите классификационные признаки компьютерных вирусов.
53. Охарактеризуйте файловый и загрузочный вирусы.
54. В чем особенности резидентных вирусов?
55. Сформулируйте признаки стелс-вирусов.
56. Перечислите деструктивные возможности компьютерных вирусов.
57. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
58. Перечислите виды «вирусоподобных» программ.
59. Поясните механизм функционирования «троянской программы» (логической бомбы).
60. В чем заключаются деструктивные свойства логических бомб?
61. Как используются утилиты скрытого администрирования и их деструктивные возможности?
62. Охарактеризуйте «intended»-вирусы и причины их появления.
63. Для чего используются конструкторы вирусов?
64. Для создания каких вирусов используются полиморфик-генераторы?
65. Поясните понятия «сканирование налету» и «сканирование по запросу».
66. Перечислите виды антивирусных программ.
67. Охарактеризуйте антивирусные сканеры.
68. Принципы функционирования блокировщиков и иммунизаторов.
69. Особенности CRC-сканеров.
70. В чем состоят особенности эвристических сканеров?
71. Какие факторы определяют качество антивирусной программы?
72. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
73. Какие особенности заражения вирусами при использовании электронной почты?
74. Особенности заражения компьютеров локальных сетей.
75. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
76. Как ограничить заражение макровирусом при работе с офисными приложениями?
77. Как обнаружить загрузочный вирус?
78. Как обнаружить резидентный вирус?
79. Характерные черты макровируса.
80. Как проверить систему на наличие макровируса?

Этапы формирования компетенций

Код формируемой компетенции	Этап формирования		
	начальный	промежуточный	завершающий
ОК-4	+		
ОПК-1	+		
ОПК-4	+		
ПК-1	+		
ПК-18		+	
ПК-21	+		
ПК-22		+	
ПК-23		+	
ПК-24	+		