МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИЖЕВСКАЯ ГОСУДАРСТВЕННАЯ СЕЛЬСКОХОЗЯЙСТВЕННАЯ АКАДЕМИЯ»

УТВЕРЖДАЮ
Проректор по учебной работе:
_____ /П.Б. Акмаров/
"11" 04 2017 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине «Информационная безопасность организации»

Специальность: «Экономическая безопасность»

Квалификация выпускника: экономист

Форма обучения - очная, заочная

Ижевск 2017

Оглавление

1 НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ

1.1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ»

Цель дисциплины «Информационная безопасность организации» заключается в изучении проблем информационной безопасности организации различных типов и направлений деятельности, построения и функционирования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности и сохранности их информационных ресурсов.

Основные задачи дисциплины:

-овладение теоретическими, практическими и методическими вопросами классификации угроз информационным ресурсам;

- ознакомление с современными проблемами информационной безопасности, основными концептуальными положениями системы защиты информации;

- изучение основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи;

- приобретение теоретических и практических навыков и способностей осуществления мероприятий по обеспечению информационной безопасности функционирования информационной системы при взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными.

В результате освоения дисциплины обучающийся должен овладеть основными требованиями, характеризующими профессиональную деятельность специалиста.

Область профессиональной деятельности специалистов-экономистов включает:

- обеспечение экономической безопасности общества, государства и личности, субъектов экономической деятельности;
- обеспечение законности и правопорядка в сфере экономики;
- судебно-экспертная деятельность по обеспечению судопроизводства, предупреждения, раскрытия и расследования правонарушений в сфере экономики;
- экономическая, социально-экономическая деятельность хозяйствующих субъектов, экономических, финансовых, производственно-экономических и аналитических служб организации, учреждений, предприятий различных форм собственности, государственных и муниципальных органов власти, конкурентная разведка;
- экономическое образование.

Объектами профессиональной деятельности специалистов являются:

- общественные отношения в сфере обеспечения законности и правопорядка, экономической безопасности;
- события и действия, создающие угрозы экономической безопасности;
- свойства и признаки материальных носителей розыскной и доказательственной информации;
- поведение хозяйствующих субъектов, их затраты, риски и результаты экономической деятельности,

- функционирующие рынки,
- финансовые и информационные потоки,
- производственные процессы.

Специалист по специальности 38.05.01 Экономическая безопасность готовится к следующим видам профессиональной деятельности:

расчетно-экономической, проектно-экономической;

контрольно-ревизионной;

информационно-аналитической;

экспертно-консультационной;

организационно-управленческой;

научно-исследовательской;

Специалист по специальности 38.05.01 Экономическая безопасность должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

в области расчетно-экономической, проектно-экономической деятельности:

- формирование системы качественных и количественных критериев экономической безопасности, индикаторов порогового или критического состояния экономических систем и объектов;

- подготовка исходных данных для проведения расчетов экономических и социально-экономических показателей, характеризующих деятельность хозяйствующих субъектов;

- проведение расчетов экономических и социально-экономических показателей на основе типовых методик с учетом действующей нормативно-правовой базы,

- разработка и обоснование системы экономических и социально-экономических показателей, характеризующих деятельность хозяйствующих субъектов;

- разработка экономических разделов планов предприятий, учреждений, организации;

- подготовка заданий и разработка проектных решений, методических и нормативных документов;

в области контрольно-ревизионной деятельности:

- контроль формирования и исполнения бюджетов бюджетной системы Российской Федерации, бюджетов государственных внебюджетных фондов, бюджетных смет, предупреждение, выявление и пресечение нарушений при формировании и использовании государственных и муниципальных ресурсов;

- оценка эффективности систем внутреннего контроля и аудита в государственных и муниципальных органах, предприятиях, организациях и учреждениях различных форм собственности;

в области информационно-аналитической деятельности:

- поиск и оценка источников информации, анализ данных, необходимых для проведения экономических расчетов;

- мониторинг текущего экономического и финансового состояния хозяйствующих субъектов на предмет надежности ресурсного потенциала, стабильности и устойчивости их деятельности;

- мониторинг экономических процессов, сбор, анализ и оценка информации, имеющей значение для обеспечения экономической безопасности; выявление экономических рисков и угроз экономической безопасности;

- обработка массивов статистических данных, экономических показателей, характеризующих социально-экономические процессы в соответствии с поставленной задачей, анализ, интерпретация, оценка полученных результатов и обоснование выводов;

- оценка экономической эффективности проектов;

- моделирование экономических процессов в целях анализа и прогнозирования угроз экономической безопасности;

- информационно-аналитическое обеспечение предупреждения, выявления, пресечения, раскрытия и расследования экономических и налоговых преступлений;

- мониторинг взаимосвязи экономических процессов и динамики правонарушений и преступлений;

в области экспертно-консультационной деятельности:

- производство судебных экономических экспертиз;

- производство исследований по заданиям правоохранительных органов и других субъектов правоприменительной деятельности;

- экспертная оценка финансово-хозяйственной деятельности предприятия, организации, учреждения с целью определения сложившейся финансовой ситуации;

- оценка факторов риска, способных создавать социально-экономические ситуации критического характера; прогноз возможных чрезвычайных социально-экономических ситуаций, разработка и осуществление мероприятий по их предотвращению или смягчению;

- оценка возможных экономических потерь в случае нарушения экономической и финансовой безопасности и определение необходимых компенсационных резервов;

- экономическая экспертиза нормативных правовых актов;

- разработка методических рекомендаций по обеспечению экономической безопасности бизнеса;

- консультирование по вопросам выявления потенциальных и реальных угроз экономической безопасности;

в области организационно-управленческой деятельности:

- организация работы малых коллективов и групп исполнителей в процессе решения конкретных профессиональных задач;

в области научно-исследовательской деятельности:

- проведение прикладных научных исследований в соответствии с профилем своей профессиональной деятельности;

2 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ», СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В процессе изучения дисциплины студент осваивает и развивает следующие компетенции:

- способностью принимать оптимальные управленческие решения с учетом критериев социально-экономической эффективности, рисков и возможностей использования имеющихся ресурсов (ПК-43);
- способностью проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации (ПК-48)

В результате изучения данной дисциплины студент должен:

Знать:

– структуру и основные положения нормативной базы РФ и национальных стандартов в области информационной безопасности и защиты информации;
– основные каналы несанкционированного доступа к информации; базовые методы и средства защиты информации от несанкционированного доступа;
– современное состояние компьютерной преступности и ответственность за нарушения и преступления в сфере информационной безопасности.

Уметь:

– ориентироваться в нормативно-правовой базе и стандартах в области информационной безопасности и защиты информации;
– идентифицировать основные угрозы безопасности ИТ-инфраструктуры современного предприятия;
– создавать защищенные учетные записи и защищать электронные документы;
– классифицировать компьютерные преступления.

Владеть:

– профессиональной терминологией в сфере информационной безопасности и защиты информации;
– проблематикой и методологией решения задач управления информационной безопасностью.

2.1 Перечень профессиональных (ПК) компетенций

Номер/индекс компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины обучающиеся должны:		
		Знать	Уметь	Владеть
ПК-43	способностью принимать оптимальные управленческие решения с учетом критериев социально-экономической эффективности, рисков и возможностей использования имеющихся ресурсов	Основы математического анализа и исследования операций в экономике. Понятие экономико-математических методов и моделей. Методы и особенности математического моделирования социально-экономических процессов и области их применения.	Составлять экономико-математические модели. Применять методы математического программирования и экономико-математического моделирования. Использовать методы теоретического и экспериментального исследования для решения экономических задач.	Методикой построения математических моделей. Методикой анализа и применения математических моделей для оценки состояния экономических субъектов. Методикой принятия оптимальных управленческих решений с учетом критериев социально-экономической эффективности и возможностей исполь-

				зования имеющихся ресурсов. Методикой прогноза развития экономических явлений и процессов.
ПК-48	способностью проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации	характеристики и свойства информационных ресурсов в условиях рыночных отношений, критерии надежности и достоверности информации; классификацию и характеристики основных методов и средств защиты информации, практику и специфику их использования по областям применения;	структурировать информационные ресурсы в соответствии с их ценностью и полезностью, определять необходимость их защиты от несанкционированного доступа;	навыками организации отбора и внедрения перспективных технических средств обеспечения информационной безопасности фирмы, охраны, сигнализации, информирования и оповещения

3 УКАЗАНИЕ МЕСТА ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ» В СТРУКТУРЕ ООП

Дисциплина «Информационная безопасность организации» включена в вариативную часть учебного плана по специальности 38.05.01, дисциплины по выбору.

В ходе изучения дисциплины большое внимание уделяется аспектам, связанным с методологическими особенностями дисциплины, которые носят собирательный, междисциплинарный и прикладной характер.

Организация изучения дисциплины предусматривает чтение лекций, проведение практических занятий, самостоятельную работу студентов по темам дисциплины.

Овладение методологией и методикой осуществления мероприятий по обеспечению информационной безопасности необходимо для изучения следующих дисциплин: «Экономическая безопасность», «Профилактика экономических преступлений», «Судебная экономическая экспертиза».

«Информационная безопасность организации» как учебная дисциплина в системе подготовки экономистов связана с дисциплинами учебного плана: «Экономическая информатика», «Информационные системы в экономике», «Программное обеспечение информационных систем», «Справочно-правовые системы».

3.1 Содержательно-логические связи дисциплины «Информационная безопасность организации»

Содержательно-логические связи	
коды и название учебных дисциплин (модулей), практик	
на которые опирается содержание данной учебной дисциплины	для которых содержание данной учебной дисциплины выступает опорой
Экономическая информатик Информационные системы в экономике Программное обеспечение информационных систем, Справочно-правовые системы Кодирование и защита информации	Экономическая безопасность Судебная экономическая экспертиза Профилактика экономических преступлений

4 ОБЪЕМ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ» В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

Вид учебной работы, часов	Очная форма	Заочная форма
	Семестр	
	6	3
1.Аудиторная работа, всего:	60	12
Лекции	20	6
Лабораторные занятия	40	6
2.Самостоятельная работа студентов (СРС):	57	123
- рефераты - контрольная работа - самоподготовка (самостоятельное изучение разделов, проработка и повторение лекционного материала, учебников и учебно-методических пособий, подготовка к практическим занятиям и пр.)	20 37	50 73
Промежуточная аттестация Экзамен	27	9
Общая трудоемкость дисциплины	144	144

4.1 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ»

4.1.1 Структура дисциплины (очная форма обучения)

№ п/п	Семестр	Недели семестра	Раздел дисциплины (модуля), темы раздела	Виды учебной работы, включая СРС и трудоемкость (в часах)						Форма: -текущего контроля успеваемости, СРС КРС
				всего	лекция	лаб. занятия	практ. занятия	семинары	СРС	
1	6	1	**Раздел 1. Концепция информационной безопасности. Нормативная база и стандарты в области информационной безопасности**	**18**	**2**	**6**			**10**	
	6	1-3	Актуальность информационной безопасности. Нормативная база информационной безопасности и защиты информации	18	2	6			10	
2	6	4	**Раздел 2. Угрозы безопасности информации**	**29**	**4**	**10**			**15**	
		4-5	Информационная безопасность сетей.	16	2	4			10	Проверка заданий, выполняемых на компьютерах
		6-8	Угрозы несанкционированного доступа к информации. Нетрадиционные информационные каналы.	13	2	6			5	Самостоятельная работа по теме
3	6	9	**Раздел 3. Методы и средства защиты информации от несанкционированного доступа**	**36**	**6**	**12**			**18**	
	6	9-10	Криптографическая защита информации	12	2	4			6	
	6	11-12	Методы и средства разграничения и контроля доступа к информации	12	2	4			6	Проверка заданий, выполняемых на компьютерах
		13-14	Системы предотвращения утечки информации из корпоративной сети	12	2	4			6	Самостоятельная работа по теме
4	6	15	**Раздел 4. Компьютерная преступность**	**12**	**4**	**4**			**4**	
	6	15-16	Компьютерная преступность. Ответственность за нарушения и преступления в сфере информационной безопасности	12	4	4			4	Проверка заданий, выполняемых на компьютерах
5	6	17	**Раздел 5. Информационная безопасность информационных систем организации**	**22**	**4**	**8**			**10**	
	6	17-20	Теория информационной безопасности информационных систем. Организация информационной безопасности кампании	22	4	8			10	
	6	20	Промежуточная аттестация	**27**						Экзамен
Итого				**144**	**20**	**40**			**57**	**27**

4.1.2 Структура дисциплины (заочная форма обучения)

№ п/п	Семестр	Недели семестра	Раздел дисциплины (модуля), темы раздела	Виды учебной работы, включая СРС и трудоемкость (в часах)						Форма: -текущего контроля успеваемости, СРС КРС
				всего	лекция	лаб. занятия	практ. занятия	семинары	СРС	
1	3		**Раздел 1. Концепция информационной безопасности. Нормативная база и стандарты в области информационной безопасности**	**19**	**1**				**18**	
	3		Актуальность информационной безопасности. Нормативная база информационной безопасности и защиты информации	19	1				18	
2	3		**Раздел 2. Угрозы безопасности информации**	**33**	**1**	**2**			**30**	
	3		Информационная безопасность сетей.	17	1	1			15	Проверка заданий, выполняемых на компьютерах
	3		Угрозы несанкционированного доступа к информации. Нетрадиционные информационные каналы.	16		1			15	Самостоятельная работа по теме
3	3		**Раздел 3. Методы и средства защиты информации от несанкционированного доступа**	**40**	**2**	**2**			**36**	
	3		Криптографическая защита информации	14	1	1			12	
	3		Методы и средства разграничения и контроля доступа к информации	14	1	1			12	Проверка заданий, выполняемых на компьютерах
	3		Системы предотвращения утечки информации из корпоративной сети	12					12	Самостоятельная работа по теме
4	3		**Раздел 4. Компьютерная преступность**	**15**		**1**			**14**	
	3		Компьютерная преступность. Ответственность за нарушения и преступления в сфере информационной безопасности	15		1			14	Проверка заданий, выполняемых на компьютерах
5	3		**Раздел 5. Информационная безопасность информационных систем организации**	**28**	**2**	**1**			**25**	
	3		Теория информационной безопасности информационных систем. Организация информационной безопасности кампании	28	2	1			25	
	3		Промежуточная аттестация	**9**						Экзамен
Итого				**144**	**6**	**6**			**123**	**9**

4.1.3 Матрица формируемых дисциплиной компетенций

Разделы и темы дисциплины	Кол-во часов	Компетенции		
		ПК-43	ПК-48	общее количество компетенций
Раздел 1. Концепция информационной безопасности. Нормативная база и стандарты в области информационной безопасности	**20**	+		1
Актуальность информационной безопасности. Нормативная база информационной безопасности и защиты информации	20	+		1
Раздел 2. Угрозы безопасности информации	**34**	+	+	2
Информационная безопасность сетей.	16	+	+	3
Угрозы несанкционированного доступа к информации. Нетрадиционные информационные каналы.	18	+	+	2
Раздел 3. Методы и средства защиты информации от несанкционированного доступа	**42**	+	+	2
Криптографическая защита информации	14	+	+	2
Методы и средства разграничения и контроля доступа к информации	14	+	+	2
Системы предотвращения утечки информации из корпоративной сети	14	+	+	2
Раздел 4. Компьютерная преступность	**12**		+	1
Компьютерная преступность. Ответственность за нарушения и преступления в сфере информационной безопасности	12		+	1
Раздел 5. Информационная безопасность информационных систем организации	**36**		+	1
Теория информационной безопасности информационных систем. Организация информационной безопасности кампании	36		+	1
Итого	144			**2**

4.1.4 Содержание разделов дисциплины «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ»

№	Название раздела	Содержание раздела в дидактических единицах
	Раздел 1. Концепция информационной безопасности. Нормативная база и стандарты в области информационной безопасности	
1	Актуальность информационной безопасности. Нормативная база информационной безопасности и защиты информации	Государственная политика в сфере информационной безопасности и защиты информации. Правовое обеспечение информационной безопасности. Конституция РФ об «информационных правах и обязанностях». Основные нормативные документы, регулирующие отношения в сфере информационной безопасности. Акты регуляторов в сфере защиты информации. Институт «тайны» в Российском законодательстве. Классификация тайн. Правовые основания отнесения сведений к категории ограниченного доступа. Краткая история защиты информации в России. Обобщенная модель информационной безопасности. Национальные стандарты в области информационной безопасности и защиты информации. Международные стандарты в области информационной безопасности и защиты информации. Проблемы гармонизации стандартов информационной безопасности.
2	**Раздел 2. Угрозы безопасности информации**	
1	Информационная безопасность сетей.	Электромагнитный спектр как источник воздействия на информацию. Классификация технических каналов утечки информации. Информационная безопасность в условиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ.
2	Угрозы несанкционированно-	Классификация угроз несанкционированного доступа к информации. Ка-

	го доступа к информации. Нетрадиционные информационные каналы.	тегории нарушителей безопасности информации и их возможности. Общая характеристика уязвимостей. Способы реализации угрозы несанкционированного доступа к информации. Понятие и обобщённая модель нетрадиционного информационного канала. Методы сокрытия информации в текстовых файлах. Методы сокрытия информации в звуковых файлах. Методы сокрытия информации в сетевых пакетах и исполняемых файлах.
3	**Раздел 3. Методы и средства защиты информации от несанкционированного доступа**	
1	Криптографическая защита информации	Модель криптосистемы. Историография и классификация шифров. Примеры криптографических алгоритмов. Криптосистема с симметричными и несимметричными ключами. Электронная цифровая подпись.
2	Методы и средства разграничения и контроля доступа к информации	Мандатная и дискреционная модели доступа. Процедура идентификации, аутентификации и авторизации. Система паролирования. Системы контроля и управления доступом. Система охраны периметра.
3	Системы предотвращения утечки информации из корпоративной сети	Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети. Понятие и функционал DLP-систем. Объем и структура данных защищаемых DLP-системами. Критерии оценки программных продуктов, реализующих функциональность DLP.
4	**Раздел 4. Компьютерная преступность**	
1	Компьютерная преступность. Ответственность за нарушения и преступления в сфере информационной безопасности	Понятие компьютерной преступности. Масштабы и общественная опасность компьютерной преступности. Виды и субъекты компьютерных преступлений. Специфика расследования компьютерных преступлений. Предупреждение компьютерных преступлений. Кодификатор Интерпола. Дисциплинарная ответственность за разглашение охраняемой законом тайны. Административная ответственность за нарушения в сфере информационной безопасности и защиты информации. Уголовная ответственность за нарушение закона о государственной тайне.
5	**Раздел 5. Информационная безопасность информационных систем организации**	
1	Теория информационной безопасности информационных систем. Организация информационной безопасности кампании	Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Организация информационной безопасности компании. Выбор средств информационной безопасности.

4.1.5 Практические занятия (не предусмотрен планом)

№ п/п	№ раздела дисциплины	Наименование практических занятий	Трудоемкость (час.)

4.1.6 Лабораторный практикум (очная форма обучения)

№ п/п	№ раздела дисциплины	Тематика лабораторных занятий	Трудоемкость (час.)
1	**Раздел 1. Концепция информационной безопасности. Нормативная база и стандарты в области информационной безопасности**		**6**
1	Актуальность информационной безопасности. Нормативная база информационной безопасности и защиты информации	Практическое занятие №1. Международные стандарты информационного обмена. Понятие угрозы	6
2	**Раздел 2. Угрозы безопасности информации**		**10**
1	Информационная безопасность сетей.	Практическое занятие № 2. Информационная безопасность в условиях функционирования в России глобальных сетей.	4
2	Угрозы несанкционированного доступа к информации. Нетрадиционные информационные каналы.	Практическое занятие № 3. Виды противников или «нарушителей». Понятие о видах вируса.	6
3	**Раздел 3. Методы и средства защиты информации от несанкционированного доступа**		**12**
1	Криптографическая защита информации	Практическое занятие № 4. Три вида возможных нарушений информационной системы. Защита.	4

2	Методы и средства разграничения и контроля доступа к информации	Практическое занятие № 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	4
3	Системы предотвращения утечки информации из корпоративной сети	Практическое занятие № 6. Модели безопасности и их применение.	4
4	**Раздел 4. Компьютерная преступность**		**4**
1	Компьютерная преступность. Ответственность за нарушения и преступления в сфере информационной безопасности	Практическое занятие № 7. Основные положения теории информационной безопасности информационных систем.	4
5	**Раздел 5. Информационная безопасность информационных систем организации**		**8**
1	Теория информационной безопасности информационных систем. Организация информационной безопасности кампании	Практическое занятие № 8. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	8
	Итого		**40**

4.1.7 Лабораторный практикум (заочная форма обучения)

№ п/п	№ раздела дисциплины	Тематика лабораторных занятий	Трудоемкость (час.)
1	**Раздел 1. Концепция информационной безопасности. Нормативная база и стандарты в области информационной безопасности**		
1	Актуальность информационной безопасности. Нормативная база информационной безопасности и защиты информации	Практическое занятие №1. Международные стандарты информационного обмена. Понятие угрозы	
2	**Раздел 2. Угрозы безопасности информации**		**2**
1	Информационная безопасность сетей.	Практическое занятие № 2. Информационная безопасность в условиях функционирования в России глобальных сетей.	1
2	Угрозы несанкционированного доступа к информации. Нетрадиционные информационные каналы.	Практическое занятие № 3. Виды противников или «нарушителей». Понятие о видах вируса.	1
3	**Раздел 3. Методы и средства защиты информации от несанкционированного доступа**		**2**
1	Криптографическая защита информации	Практическое занятие № 4. Три вида возможных нарушений информационной системы. Защита.	1
2	Методы и средства разграничения и контроля доступа к информации	Практическое занятие № 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	1
4	**Раздел 4. Компьютерная преступность**		**1**
1	Компьютерная преступность. Ответственность за нарушения и преступления в сфере информационной безопасности	Практическое занятие № 7. Основные положения теории информационной безопасности информационных систем.	1
5	**Раздел 5. Информационная безопасность информационных систем организации**		**1**
1	Теория информационной безопасности информационных систем. Организация информационной безопасности кампании	Практическое занятие № 8. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	1
	Итого		**6**

4.1.8 Содержание самостоятельной работы и формы ее контроля (очная форма обучения)

№ п/п	Раздел дисциплины (модуля), темы раздела	Всего часов	Содержание самостоятельной работы	Форма контроля
1	**Раздел 1. Концепция информационной безопасности. Нормативная база и стандарты в области информационной безопасности**			
1	Актуальность информационной безопасности. Нормативная база информационной безопасности и защиты информации	10	Работа с учебной литературой, подготовка к лекции	Проверка заданий, выполняемых на компьютерах
4	**Раздел 2. Угрозы безопасности информации**			
4	Информационная безопасность сетей.	10	Работа с учебной литературой. Решение задач из практикума по эконометрике.*	Проверка заданий, выполняемых на компьютерах
5	Угрозы несанкционированного доступа к информации. Нетрадиционные информационные каналы.	5	Работа с учебной литературой.	Самостоятельная работа по теме.
12	**Раздел 3. Методы и средства защиты информации от несанкционированного доступа**			
12	Криптографическая защита информации	6	Работа с учебной литературой.	Проверка заданий, выполняемых на компьютерах
13	Методы и средства разграничения и контроля доступа к информации	6	Решение задач из практикума по эконометрике.*	
14	Системы предотвращения утечки информации из корпоративной сети	6	Работа с учебной литературой.	Самостоятельная работа по теме
12	**Раздел 4. Компьютерная преступность**			
12	Компьютерная преступность. Ответственность за нарушения и преступления в сфере информационной безопасности	4	Решение задач из практикума по эконометрике. *	Проверка заданий, выполняемых на компьютере
12	**Раздел 5. Информационная безопасность информационных систем организации**			
12	Теория информационной безопасности информационных систем. Организация информационной безопасности кампании	10	Работа с учебной литературой, решение задач из практикума по эконометрике. Подготовка к зачетному тестированию.	Проверка заданий, выполняемых на компьютере.
		57		

4.1.9 Содержание самостоятельной работы и формы ее контроля (заочная форма обучения)

№ п/п	Раздел дисциплины (модуля), темы раздела	Всего часов	Содержание самостоятельной работы	Форма контроля
1	**Раздел 1. Концепция информационной безопасности. Нормативная база и стандарты в области информационной безопасности**			
1	Актуальность информационной безопасности. Нормативная база информационной безопасности и защиты информации	18	Работа с учебной литературой, подготовка к лекции	Проверка заданий, выполняемых на компьютерах
4	**Раздел 2. Угрозы безопасности информации**			
4	Информационная безопасность сетей.	15	Работа с учебной литературой. Решение задач из практикума по эконометрике.*	Проверка заданий, выполняемых на компьютерах
5	Угрозы несанкционированного доступа к информации. Нетрадиционные информационные каналы.	15	Работа с учебной литературой.	Самостоятельная работа по теме.
12	**Раздел 3. Методы и средства защиты информации от несанкционированного доступа**			
12	Криптографическая защита информации	12	Работа с учебной литературой.	Проверка заданий, выполняемых на компьютерах
13	Методы и средства разграничения и	12	Решение задач из практикума по	

	контроля доступа к информации		эконометрике.*	
14	Системы предотвращения утечки информации из корпоративной сети	12	Работа с учебной литературой.	Самостоятельная работа по теме
12	**Раздел 4. Компьютерная преступность**			
12	Компьютерная преступность. Ответственность за нарушения и преступления в сфере информационной безопасности	14	Решение задач из практикума по эконометрике. *	Проверка заданий, выполняемых на компьютере
12	**Раздел 5. Информационная безопасность информационных систем организации**			
12	Теория информационной безопасности информационных систем. Организация информационной безопасности кампании	25	Работа с учебной литературой, решение задач из практикума по эконометрике. Подготовка к зачетному тестированию.	Проверка заданий, выполняемых на компьютере.
		123		

5 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Применение мультимедийного оборудования на лекциях, компьютерных программ MICROSOFT OFFICE на практических занятиях и для самостоятельной работы.

5.1 Интерактивные образовательные технологии, используемые в аудиторных занятиях

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
	Л	Курс лекций читается с использованием мультимедийных материалов	20
Итого			20

6 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Контроль знаний студентов по дисциплине «Информационная безопасность организации» проводится в устной и письменной форме, предусматривает текущий, промежуточный и итоговый контроль (экзамен).

Методы контроля:

- тестовая форма контроля;
- устная форма контроля – опрос и общение с аудиторией по поставленной задаче в устной форме;
- решение определенных заданий (задач) по теме практического материала в конце практического занятия, в целях эффективности усвояемости материала на практике.
- использование ролевых игр (соревнований) по группам, внутри групп;
- поощрение индивидуальных заданий, в которых студент проработал самостоятельно большое количество дополнительных источников литературы.

Текущий контроль предусматривает устную форму опроса студентов и письменный экспресс-опрос по окончанию изучения каждой темы.

Промежуточная аттестация - экзамен**.**

6 Виды контроля и аттестации, формы оценочных средств

№ п/п	№ семестра	Виды контроля и аттестации (ВК, ТАт, ПрАт)	Наименование раздела учебной дисциплины (модуля)	Оценочные средства
1.	6	ВК	**Раздел 1. Концепция информационной безопасности. Нормативная база и стандарты в области информационной безопасности**	входной контроль
2.	6	ТАт	**Раздел 2. Угрозы безопасности информации**	самостоятельная работа
3.	6	ТАт	**Раздел 3. Методы и средства защиты информации от несанкционированного доступа**	самостоятельная работа
	6	ТАт	**Раздел 4. Компьютерная преступность**	тестирование по разделу
	6	ТАт	**Раздел 5. Информационная безопасность информационных систем организации**	тестирование по разделу
4.	6	ПрАТ	Экзамен	тестирование по итогам курса

*Фонд оценочных средств для промежуточной аттестации приведен в приложении к рабочей программе.

Вопросы к экзамену по дисциплине
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ»

1. Понятие информационной безопасности. Основные составляющие.
2. Основные определения и критерии классификации угроз.
3. Вредоносное программное обеспечение.
4.Основные угрозы целостности. Основные угрозы конфиденциальности.

5.Законодательный уровень информационной безопасности.
6. Обзор российского законодательства в области информационной безопасности.
7. Закон «Об информации, информатизации и защите информации».
8. Закон «О лицензировании отдельных видов деятельности».
9. Обзор зарубежного законодательства в области информационной безопасности.
10. Стандарты и спецификации в области информационной безопасности.
11. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт.
12. Механизмы безопасности.
13. Классы безопасности.
14. Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности.
15. Сетевые механизмы безопасности.
16. Администрирование средств безопасности.
17. О необходимости объектно-ориентированного подхода к информационной безопасности.
18. Основные понятия объектно-ориентированного подхода.
19. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.
20. Административный уровень информационной безопасности. Основные понятия.
21. Административный уровень информационной безопасности. Политика безопасности.
22. Административный уровень информационной безопасности. Программа безопасности.
23. Административный уровень информационной безопасности. Синхронизация программы безопасности с жизненным циклом систем.
24. Управление рисками. Основные понятия.
25. Подготовительные этапы управления рисками.
26. Основные этапы управления рисками.
27. Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня.
28. Процедурный уровень информационной безопасности. Управление персоналом.
29. Процедурный уровень информационной безопасности. Физическая защита.
30. Процедурный уровень информационной безопасности. Поддержание работоспособности.
31. Процедурный уровень информационной безопасности. Реагирование на нарушение режима безопасности.
32. Процедурный уровень информационной безопасности. Планирование восстановительных работ.
33. Основные понятия программно-технического уровня информационной безопасности.
34. Архитектурная безопасность.
35. Идентификация и аутентификация. Парольная аутентификация.
36. Управление доступом. Ролевое управление доступом.
37. Управление доступом в Java-среде
38. Возможный подход к управлению доступом в распределенной объектной среде.

6.2 Перечень учебно-методического обеспечения для самостоятельной работы

1. Рабочая программа дисциплины «Информационная безопасность организации»
2. Разработки для выполнения практических заданий.
3. Задания, приведенные в литературе и порядок их выполнения (по заданию преподавателя.

7 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ»

7.1 Основная литература

№ п/п	Наименование	Автор(ы)	Год и место издания	Используется при изучении разделов	Количество экземпляров
1	Информационная безопасность и защита информации в компьютерных системах. Ч. 1. Основы криптографии : учеб. пособие	А.С. Овсянников, М.А. Бурова	Самара : Изд-во ПГУТИ, 2011	1-5	ЭБС «РУКОНТ» http://rucont.ru/efd/319810
2	Экономическая информатика. Ч. II. Прикладные программные средства. Технология создания программ. Языки программирования. Компьютерные сети. Информационная глобальная сеть Интернет. Информационная безопасность: учебное пособие.	Колганов, Е. А. , Н.Р. Сагманова	Уфим. гос. ун-т экономики и сервиса, Финансовый ун-т при Правительстве РФ (Уфим. ф-л), — Уфа : УГУЭС, 2014 .— ISBN 978-5-88469-667-9	1-5	ЭБС «РУКОНТ» http://rucont.ru/efd/314971

7.2 Дополнительная литература

№ п/п	Наименование	Автор(ы)	Год и место издания	Используется при изучении разделов	Семестр	Количество экземпляров	
						в библиотеке	на кафедре
1	Информационная безопасность и защита информации в компьютерных системах : метод. указания	Овсянников, А.С., Бурова М.А.	Самара : Изд-во ПГУТИ/—, 2011	1-5	ЭБС «РУКОНТ» http://rucont.ru/efd/319811		
2	Методы проектирования систем технической охраны объектов: учебное пособие: Направление подготовки 090900.62 (10.03.01) – Информационная безопасность. Профиль подготовки «Комплексная защита объектов информатизации». Бакалавриат	Мулкиджанян, П. П., Айвазов Ю. Г., Родишевский В. В., Макаров А. М.	Ставрополь : изд-во СКФУ, 2015	1-5	ЭБС «РУКОНТ» http://rucont.ru/efd/304156		
3	Информационная безопасность : учебное пособие	Петров, С.В., Кисляков П.А.	М. : Издательство "Русский журнал", 2011 .— ISBN 978-5-86229-295-4	1-5	ЭБС «РУКОНТ» http://rucont.ru/efd/304393		
4	Информационные технологии в образовании: учебное пособие: Направление подготовки 230400.62 – Информационные системы и технологии. Профиль подготовки «Информационная безопасность». Бакалавриат	Журавлев В. В.	.— Ставрополь : изд-во СКФУ, 2014 .— Библиогр.: с. 100	1-5	ЭБС «РУКОНТ» http://rucont.ru/efd/314107		

7.3 Перечень Интернет-ресурсов

В ресурсах Интернет

Журналы по экономическим наукам - http://www.medien.ru/ekonomicheskie-zhurnaly#ego1

Сайт Министерства экономического развития РФ - http://www.economy.gov.ru/minec/main

Сайт Министерства экономики УР - http://economy.udmurt.ru/

Сайт по вопросам информационной безопасности http://bezopasnik.org/article/1.htm

7.4 Методические указания по освоению дисциплины

Перед изучением дисциплины студенту необходимо ознакомиться с рабочей программой дисциплины, размещенной на портале и просмотреть основную литературу, приведенную в рабочей программе в разделе «Учебно-методическое и информационное обеспечение дисциплины». Книги, размещенные в электронно-библиотечных системах доступны из любой точки, где имеется выход в «Интернет», включая домашние компьютеры и устройства, позволяющие работать в сети «Интернет». Если выявили проблемы доступа к указанной литературе, обратитесь к преподавателю (либо на занятиях, либо через портал академии).

Для изучения дисциплины необходимо иметь чистую тетрадь, объемом не менее 48 листов для выполнения заданий. Перед началом занятий надо бегло повторить материал из курсов дисциплин «Экономическая информатика», «Информационные системы в экономике», «Программное обеспечение информационных систем», «Кодирование и защита информации».

Для эффективного освоения дисциплины рекомендуется посещать все виды занятий в соответствии с расписанием и выполнять все домашние задания в установленные преподавателем сроки. В случае пропуска занятий по уважительным причинам, необходимо подойти к преподавателю и получить индивидуальное задание по пропущенной теме.

Полученные знания и умения в процессе освоения дисциплины студенту рекомендуется применять для решения своих задач, не обязательно связанных с программой дисциплины. Владение компетенциями дисциплины в полной мере будет подтверждаться Вашим умением ставить конкретные задачи по разработке эконометрических моделей, а также выявлять существующие проблемы.

Полученные при изучении дисциплины знания, умения и навыки рекомендуется использовать при выполнении курсовых и дипломных работ (проектов), а также на учебных и производственных практиках.

7.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) «Информационная безопасность организации», включая перечень программного обеспечения и информационных справочных систем.

Поиск информации в глобальной сети Интернет

Работа в электронно-библиотечных системах

Работа в ЭИОС вуза (работа с порталом и онлайн-курсами в системе moodle.izhgsha.ru)

Мультимедийные лекции

Работа в компьютерном классе

Компьютерное тестирование

При изучении учебного материала используется комплект лицензионного программного обеспечения следующего состава:

1. Операционная система: Microsoft Windows 10 Professional. Подписка на 3 года. Договор № 9-БД/19 от 07.02.2019. Последняя доступная версия программы. Astra Linux Common Edition. Договор №173-ГК/19 от 12.11.2019 г.
2. Базовый пакет программ Microsoft Office (Word, Excel, PowerPoint). Microsoft Office Standard 2016. Бессрочная лицензия. Договор №79-ГК/16 от 11.05.2016. Microsoft Office Standard 2013. Бессрочная лицензия. Договор №0313100010014000038-0010456-01 от 11.08.2014. Microsoft Office Standard 2013. Бессрочная лицензия. Договор №26 от 19.12.2013. Microsoft Office Professional Plus 2010. Бессрочная лицензия. Договор №106-ГК от 21.11.2011. Р7-Офис. Договор №173-ГК/19 от 12.11.2019 г.
3. Информационно-справочная система (справочно-правовая система) «Консультант плюс». Соглашение № ИКП2016/ЛСВ 003 от 11.01.2016 для использования в учебных целях бессрочное. Обновляется регулярно. Лицензия на все компьютеры, используемые в учебном процессе.
4. Программное обеспечение (профессиональные базы данных) на платформе 1С: Предприятие с доступными конфигурациями (1С: ERP Агропромышленный комплекс 2, 1С: ERP Энергетика, 1С: Бухгалтерия молокозавода, 1С: Бухгалтерия птицефабрики, 1С: Бухгалтерия элеватора и ком-бикормового завода, 1С: Общепит, 1С: Ресторан. Фронт-офис). Лицензионный договор № Н8775 от 17.11.2020 г.

8 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ) «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ»

Тип аудитории	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы
Лекции	Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Компьютерный класс, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: компьютеры с необходимым программным обеспечением, выходом в «Интернет» и корпоративную сеть ВУЗа.
Практики (компьютерный класс)	Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (лаборатория). Компьютерный класс, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: компьютеры с необходимым программным обеспечением, выходом в «Интернет» и корпоративную сеть ВУЗа.
Самостоятельная работа	Помещение для самостоятельной работы. (читальный зал №4) Помещение оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.

ПРИЛОЖЕНИЕ 1

ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Информационная безопасность организации»
(приложение к рабочей программе дисциплины)

1.ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Название раздела	Код контролируемой компетенции (или её части)	Оценочные средства для проверки знаний (1-й этап)	Оценочные средства для проверки умений (2-й этап)	Оценочные средства для проверки владений (навыков) (3-й этап)
Раздел 1. Концепция информационной безопасности. Нормативная база и стандарты в области информационной безопасности	ПК-43	Вопросы к контрольной работе 1-4	Вопросы для самопроверки 1-15	Тестовые задания Вопросы к экзамену 1-6
Раздел 2. Угрозы безопасности информации	ПК-48	Вопросы к контрольной работе 5-18	Вопросы для самопроверки 16-30	Тестовые задания Вопросы к экзамену 7-17
Раздел 3. Методы и средства защиты информации от несанкционированного доступа	ПК-43	Вопросы к контрольной работе 19-37	Вопросы для самопроверки 31-45	Тестовые задания Вопросы к экзамену 20-32
Раздел 4. Компьютерная преступность	ПК-43, ПК-48	Вопросы к контрольной работе 38-40	Вопросы для самопроверки 46-60	Тестовые задания Вопросы к экзамену 18-19
Раздел 5. Информационная безопасность информационных систем организации	ПК-48	Вопросы к контрольной работе 41	Вопросы для самопроверки 61-75	Тестовые задания Вопросы к экзамену 33-36

2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 2.1 – Перечень компетенций

Номер/индекс компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины обучающиеся должны:		
		Знать	Уметь	Владеть
ПК-43	способностью принимать оптимальные управленческие решения с учетом критериев социально-экономической эффективности, рисков и возможностей использования имеющихся ресурсов	Основы математического анализа и исследования операций в экономике. Понятие экономико-математических методов и моделей. Методы и особенности математического моделирования социально-экономических процессов и области их применения.	Составлять экономико-математические модели. Применять методы математического программирования и экономико-математического моделирования. Использовать методы теоретического и экспериментального исследования для решения экономических задач.	Методикой построения математических моделей. Методикой анализа и применения математических моделей для оценки состояния экономических субъектов. Методикой принятия оптимальных управленческих решений с учетом критериев социально-экономической эффективности и возможностей исполь-

				зования имеющихся ресурсов. Методикой прогноза развития экономических явлений и процессов.
ПК-48	способностью проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации	характеристики и свойства информационных ресурсов в условиях рыночных отношений, критерии надежности и достоверности информации; классификацию и характеристики основных методов и средств защиты информации, практику и специфику их использования по областям применения;	структурировать информационные ресурсы в соответствии с их ценностью и полезностью, определять необходимость их защиты от несанкционированного доступа;	навыками организации отбора и внедрения перспективных технических средств обеспечения информационной безопасности фирмы, охраны, сигнализации, информирования и оповещения

3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

3.1 Описание показателей, шкал и критериев оценивания компетенций

Показателями уровня освоенности компетенций на всех этапах их формирования являются:

1-й этап (уровень знаний):

– Умение отвечать на основные вопросы и тесты на уровне понимания сути – удовлетворительно (3).

- Умение грамотно рассуждать по теме задаваемых вопросов – хорошо (4)

- Умение формулировать проблемы по сути задаваемых вопросов – отлично (5)

2-й этап (уровень умений):

- Умение решать простые задачи с незначительными ошибками - удовлетворительно (3).

- Умение решать задачи средней сложности – хорошо (4).

- Умение решать задачи повышенной сложности, самому ставить задачи – отлично (5).

3-й этап (уровень владения навыками):

- Умение формулировать и решать задачи из разных разделов с незначительными ошибками - удовлетворительно (3).

- Умение находить проблемы, решать задачи повышенной сложности – хорошо (4).

- Умение самому ставить задачи, находить недостатки и ошибки в решениях – отлично (5).

3.2 Методика оценивания уровня сформированности компетенций в целом по дисциплине

Уровень сформированности компетенций в целом по дисциплине оценивается на основе результатов текущего контроля знаний в процессе освоения дисциплины – как средний балл результатов текущих оценочных мероприятий в течение семестра;

на основе результатов промежуточной аттестации – как средняя оценка по ответам на вопросы к экзамену и решению задач;

по результатам участия в научной работе, олимпиадах и конкурсах.

Оценка выставляется по 4-х бальной шкале – неудовлетворительно (2), удовлетворительно (3), хорошо (4), отлично (5).

4.Типовые контрольные задания тесты и вопросы

Вопросы к контрольной работе

1. Информационная безопасность в системе национальной безопасности
2. Понятийный аппарат и основы терминологии информационной и национальной безопасности.
3. Виды национальной безопасности и их краткая характеристика.
4. Системные связи информационной безопасности с другими видами национальной безопасности.
5. Информационные уязвимости объектов.
6. Антропогенные информационные уязвимости.
7. Техногенные информационные уязвимости.
8. Организационно-правовые информационные уязвимости.
9. Комбинированные информационные уязвимости
10. Угрозы информационной безопасности и их источники.
11. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.

12. Эндогенные и экзогенные, угрозы информационной безопасности, их классификация.
13. Антропогенные и техногенные угрозы информационной безопасности, их классификация.
14. Системная классификация угроз информационной безопасности.
15. Угрозы конфиденциальности, целостности и доступности информации.
16. Информационная война как высшая форма угрозы информационной безопасности.
17. Категорирование информации.
18. Допуск к информационным ресурсам.
19. Основные принципы защиты информации от несанкционированного доступа.
20. Средства обеспечения информационной безопасности.
21. Аппаратные средства обеспечения информационной безопасности.
22. Программные средства обеспечения информационной безопасности.
23. Криптографические средства обеспечения информационной безопасности.
24. Стеганографические средства обеспечения информационной безопасности.
25. Организационно-правовые средства обеспечения информационной безопасности,
26. Государственная политика в области информационной безопасности.
27. Государственные органы обеспечения информационной безопасности.
28. Приоритетные направления обеспечения информационной безопасности в условиях информационного общества.
29. Приоритетные проблемы обеспечения информационной безопасности в условиях информационного общества.
30. Технические каналы утечки конфиденциальной информации. Основные методы защиты.
31. Пассивные средства противодействия техническим разведкам.
32. Активные средства противодействия техническим разведкам.
33. Базовые стратегии организации защиты информации.
34. Полное множество функций защиты информации.
35. Задачи защиты информации. Репрезентативное множество задач защиты.
36. Формирование политики обеспечения информационной безопасности объекта.
37. Проектирование оптимальных систем защиты информации.
38. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения.
39. Риски информационной безопасности
40. Статистика инцидентов информационной безопасности.
41. Основные макропроцессы управления функционированием комплексной системы защиты информации.

Вопросы для самопроверки

1. Были ли в вашей практике случаи попыток несанкционированного получения информации, обрабатываемой в АС? Охарактеризуйте проявившийся в каждом конкретном случае канал несанкционированного доступа и оцените возможную уязвимость информации.

2. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.

3. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.

4. Рассмотрите возможности несанкционированного получения информации в следующем случае:

- в рассматриваемой АС возможны нарушители двух категорий: внешние, не имеющие отношения к системе, и внутренние, входящие в состав персонала, обслуживающего АС;
- в качестве компонентов, являющихся объектами несанкционированных действий, рассматриваются магнитные носители информации (дискеты), видеотерминалы ввода-вывода информации и принтеры;
- каналами несанкционированного получения информации являются непосредственное хищение носителей, просмотр информации на экране дисплея и выдача ее на печать.

Каковы, с вашей точки зрения, в этом случае вероятности несанкционированного получения информации?

5. В чем, с вашей точки зрения, состоит опасность разработки и применения информационного оружия? Какие необходимо было бы применить меры международного характера в целях предотвращения информационных войн?

6. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?

7. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации? Рассмотрите все возможные ситуации и последствия, к которым приведут принимаемые решения по доступу с точки зрения обеспечения безопасности информации.

8. Сравните различные известные вам модели защиты от несанкционированного доступа к информации.

9. Что можно сказать о взаимодействии уровней безопасности субъектов и объектов доступа для различных видов доступа, с которыми оперирует модель Белла – Ла Падула?

10. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?

11. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?

12. Приведите примеры известных вам систем аутентификации, построенных по принципу «пользователь имеет». Что вы можете сказать о преимуществах и недостатках методов аутентификации пользователей пластиковых карт, широко используемых в банковской сфере?

13. Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик.

14. Какие основные методы контроля доступа используются в современных автоматизированных системах? Охарактеризуйте эти методы и рассмотрите их возможности для реализации автоматизированной системы ведения текущих счетов клиентов банка.
15. Охарактеризуйте процесс развития проблемы защиты информации в современных системах ее обработки.

16. Раскройте содержание разграничения доступа к информации с помощью монитора обращений.

17. Охарактеризуйте проблему определения предметной области информационной безопасности и дайте определения основным понятиям, используемым в этой сфере.

18. Раскройте содержание исторических этапов развития подходов к защите информации и обеспечению информационной безопасности.

19. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности.

20. Раскройте содержание модели разграничения доступа Лэмпсона – Грэхема – Деннинга.

21. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа.

22. В чем состоит суть принципов достаточной глубины контроля и разграничения потоков информации как основных принципов защиты информации от несанкционированного доступа?

23. Раскройте содержание принципов чистоты повторно используемых ресурсов и целостности средств защиты как основных принципов защиты информации от несанкционированного доступа.

24. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.

25. Рассмотрите основные методы повышения стойкости парольных систем аутентификации пользователей автоматизированных систем.

26. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.
27. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?

28. Объясните, что представляет собой стеганография?

29. Расскажите об особенностях симметричных и несимметричных шифров. Попробуйте привести примеры этих способов шифрования.

30. Объясните, почему основными требованиями, предъявляемыми к криптосистемам, являются наличие очень большого числа возможных ключей и равная вероятность их генерации.

31. От каких основных свойств криптографических алгоритмов зависит, на ваш взгляд, стойкость криптосистемы?

32. В чем принципиальное различие оценки стойкости криптосистемы с использованием теории информации и теории вычислительной сложности?

33. Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?

34. Опишите наиболее известный алгоритм шифрования DES. Какие из основных методов шифрования использованы в этом алгоритме?

35. Каковы основные особенности криптосистем с общедоступным ключом?

36. Раскройте основное содержание алгоритма электронной цифровой подписи.

37. Какие методы распределения ключей в криптографических системах с большим числом абонентов вы знаете? Охарактеризуйте основные особенности децентрализованных и централизованных систем.

38. Опишите последовательность установления связи и передачи сообщений в централизованных системах распределения ключей шифрования с центром трансляции ключей и с центром распределения ключей.

39. В каких случаях применяются криптографические методы защиты информации непосредственно в ЭВМ?
40. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютеров вирусами.

41. Попробуйте изобразить структуру компьютерного вируса в виде программы, написанной на псевдоязыке.

42. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.

43. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?

44. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?

45. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.

46. Рассмотрите возможности вирусного подавления как одной из форм радиоэлектронной борьбы.

47. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?

48. Раскройте содержание комплексной стратегии защиты, ориентированной на противодействие возможному вирусному подавлению.

49. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.

50. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.

51. Дайте классификацию источников утечки информации по техническим каналам.

52. Что такое основные и вспомогательные технические средства автоматизированной системы? Приведите примеры и рассмотрите возможности их использования в качестве технических каналов утечки информации.
53. Назовите известные вам методы и средства контроля акустической информации.

54. Охарактеризуйте методы контроля информации техническими средствами в каналах телефонной связи.

55. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.

56. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.

57. Приведите известные вам методы защиты от утечки информации по акустическому каналу. Попробуйте сравнить их, используя критерий «эффективность/стоимость».

58. Охарактеризуйте существующие на сегодняшний день способы защиты информации в каналах связи.

59. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.

60. С чем, по вашему мнению, связана необходимость организационно-правового обеспечения защиты информации? в чем заключается специфика этого обеспечения применительно к информации, обрабатываемой в автоматизированных системах?

61. Охарактеризуйте задачи, решаемые организационно-правовым обеспечением защиты информации в АС. Выделите особенности, связанные с «электронной» формой представления информации в АС.

62. Сформулируйте основные направления развития организационно-правового обеспечения защиты информации в зарубежных странах. Назовите известные вам законодательные акты зарубежных стран в области регулирования процессов информатизации и обеспечения безопасности информации.

63. Что вы знаете из истории развития организационно-правового обеспечения зашиты информации в СССР и Российской Федерации?
Охарактеризуйте современное состояние отечественной законодательной базы в области информатизации и защиты информации.

64. Сформулируйте основные положения Закона Российской Федерации «Об информации, информационных технологиях и защите информации». Какие еще вы знаете российские законодательные акты в этой области?

65. Сформулируйте основные подходы к разработке организационно-правового обеспечения защиты информации. Раскройте содержание структуры этого обеспечения.

66. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации. Назовите известные вам системы стандартов в этой области, принятые в России и за рубежом.

67. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности.

68. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.

69. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность? Каким требованиям должна удовлетворять концепция комплексной защиты?

70. Сформулируйте основные концептуальные положения теории защиты информации.

71. Раскройте содержание функции защиты информации. Какие из функций образуют полное множество функций защиты?

72. Сформулируйте определение задачи защиты информации и попытайтесь назвать десять классов задач, образующих репрезентативное множество задач защиты.
73. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?

74. Дайте определение системы защиты информации и сформулируйте основные концептуальные требования, предъявляемые к ней.

75. Раскройте содержание концепции управления системой защиты информации. Каковы ее особенности по сравнению с общей концепцией управления системами организационно-технологического типа?

ВАРИАНТ ТЕСТА ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ»

1. Задание.
В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?

1. 1988
2. 1991
3. 1994
4. 1997
5. 2002

2. Задание.
Сертификации подлежат:

1. средства криптографической защиты информации;
2. средства выявления складных устройств и программных закладок;
3. защищенные технические средства обработки информации;
4. защищенные информационные системы и комплексы телекоммуникаций;
5. Все вышеперечисленные средства.

3. Задание.
В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

1. Индивидуальные объекты должны идентифицироваться;
2. Контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. Необходимо имеbть явную и хорошо определенную систему обеспечения безопасности;
4. Вычислительная система в своем составе должна иметь аппаратные/ программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. Гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

4. Задание.
Естественные угрозы безопасности информации вызваны:

1. Деятельностью человека;
2. Ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. Воздействия объективных физических- процессов или стихийных природных явлений, не зависящих от человека;
4. Корыстными устремлениями злоумышленников;
5. Ошибками при действиях персонала.

5. Задание.
Хакер – это:

1. Лицо которое взламывает интрасеть в познавательных целях;
2. Мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. Лицо изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
4. Плохой игрок в гольф, дилетант;
5. Мошенник, который обманным путем выманивает у доверчивых пользователей сети конфиденциальную информацию.

6. Задание.
Активный перехват информации это – перехват, который:

1. Заключается в установке прослушивающего 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.

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

1. Черный пиар;
2. Фишинг;
3. Нигерийские письма;
4. Источник слухов;
5. Пустые письма.

8. Задание.
По среде обитания классические вирусы разделяются:

1. На паразитические;
2. На компаньоны;
3. На файловые;
4. На ссылки;
5. На перезаписывающие.

9. Задание.
Шифрование методом постановки:

1. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. Символы шифруемого текста последовательно складываются символами некоторой специальной последовательности;
3. Шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
5. Замена слов и предложений исходной информации шифрованными.

10. Задание.

Методы защиты информации ограничение доступа заключается:

1. В контроле доступа к внутреннему монтажу, линиями связи и технологическими органами управления;
2. В создании физической замкнутой преграды с организацие й доступа лиц, связанных с объектом функциональными обязанностями;
3. В разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями;
4. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. В проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

11. Задание.

Перехват, который неправомерно использует технологические отходы информационного процесса, называется:

1. Активный перехват;
2. Пассивный перехват;
3. Аудиоперехват;
4. Видеоперехват;
5. Просмотр мусора.

12. Задание.

Спам, периодически проводящий рассылки не рекламных сообщений:

1. Черный пиар;
2. Фишинг;
3. Нигерийские письма;
4. Источник слухов;
5. Пустые письма.

13. Задание.

Способ защиты информации, существующей в виде электромагнитного сигнала, зависит от:

1. Среда распространения электромагнитного сигнала;
2. Длина волны сигнала;
3. Наличия или отсутствия специальной линии связи;
4. Типа линии связи;
5. Форм воздействия на информацию или ее носитель;
6. Предполагаемого способа нападения на информацию.

14. Задание.

Попытка одного субъекта выдать себя за другого – это

1. Пассивная атака;
2. Модификация потока данных;
3. Фальсификация;
4. Повторное использование;
5. Отказ в обслуживании.

15. Задание.
В качестве биометрических признаков, которые могут быть использованы при идентификации субъекта доступа, можно выделить:

1. Должностное лицо;
2. Терминал;
3. Распечатка;
4. Форма и размер лица;
5. Оператор.

16. Задание.
Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:

1. Детектор;
2. Доктор;
3. Сканер;
4. Ревизор;
5. Сторож.

Вопросы к экзамену по дисциплине
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ»

Вопросы к экзамену

1. Понятийный аппарат и основы терминологии информационной и национальной безопасности**.**

2. Методики составления обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности;

3. Виды национальной безопасности и их краткая характеристика.

4. Проблема социальной значимости профессии, высокой мотивации к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

5. Системные связи информационной безопасности с другими видами национальной безопасности

6. Определение места и роли информационной безопасности в системе национальной безопасности России.

7. Антропогенные информационные уязвимости.

8. Методика изучения и обобщения опыта работы других учреждений, организации и предприятий в области повышения эффективности защиты информации.

9. Техногенные информационные уязвимости.

10. Проблема технических каналов утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.

11. Организационно-правовые и комбинированные информационные уязвимости.

12. Проблема использования естественнонаучных законов и применения математического аппарата в профессиональной деятельности при выявлении сущности проблем, возникающих в задачах обеспечения информационной безопасности.

13. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.

14. Проблема определения видов и форм информации, подверженной угрозам, видов, возможных методов и путей реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.

15. Угрозы, целостности, доступности и конфиденциальности информации.

16. Классификация правонарушений в сфере компьютерной информации.

17. Роль информации в развитии современного общества, применение достижений информатики и вычислительной техники в задачах переработки больших объемов информации и проведения целенаправленного поиска в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных сетях,

18. Противодействия нарушениям конфиденциальности, целостности и доступности информации и киберпреступности.

19. Информационная война как высшая форма угрозы информационной безопасности.

20. Проблема применения методов и средств выявления угроз безопасности автоматизированным системам.
21. Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам.

22. Проблема применения методик проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности.

23. Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности.

24. Проблема разработки методик проведения совместного анализа функционального процесса объекта защиты и применяемых информационных технологий и технических средств с целью определения возможных источников информационных угроз, их вероятных целей и тактики.

25. Пассивные и активные средства противодействия техническим разведкам, информационное противоборство.

26. Применение принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.

27. Статистика инцидентов информационной безопасности.

28. Проблема применения принципов и методов анализа и оценки угроз информационной безопасности объекта.

29. Проблема применения методов формирования требований по защите информации по критерию цена-качество.

30. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения.

31. Проблемам разработки методик применения комплексного подхода к обеспечению информационной безопасности в различных сферах деятельности.

32. Проблема применения принципов и методов анализа и оценки угроз информационной безопасности.
33. Государственные органы обеспечения информационной безопасности.

34. Применение основных нормативных правовых актов в области информационной безопасности и защиты информации, а также нормативных методических документов ФСБ России, ФСТЭК России в данной области.

35. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного общества.

36. Проблема стимулирования готовности и способности к активной состязательной деятельности при решении задач обеспечения информационной безопасности в условиях информационного противоборства.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номер измененного листа	Дата внесения изменения и номер протокола	Подпись ответственного за внесение изменений
1	18-22	27.08.18 № 1	
2	18-22	30.08.19 № 1	
3	18-22	29.08.20 № 1	
4	21	20.11.20 № 3	
5	21	31.08.21 № 1	
6			