МОДУЛЬ 1. МЕСТО ИБ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Тема 1: ВВЕДЕНИЕ

ВОПРОСЫ

1. **ПРОГРАММЫ ВПО В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**
2. **СОЦИАЛЬНАЯ ЗНАЧИМОСТЬ ПРОФЕССИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**
3. **ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ БАКАЛАВРОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».**
4. **ПРОГРАММА ДИСЦИПЛИНЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».**

Литература:1. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. Алт.гос. техн.ун-т им.И.И.Ползунова.- Баранаул: -2011-253с. (60 экз.Гриф УМО)

2. Организационно – правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / А.А.Стрельцов [и др.]; под ред.А.А. Стрельцова.- М.: Издательский центр «Академия», 2008.-256с.

1 ПРОГРАММЫ ВПО В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки бакалавров «Информационная безопасность»

Код направления	Профили	срок	квалиф
10.03.01	***Компьютерная безопасность***	4	бакалавр
	Безопасность телекоммуникационных сетей	4	бакалавр
	Комплексная защита объектов информатизации	4	бакалавр
	Безопасность автоматизированных систем	4	бакалавр
	Организация и технология защиты информации		
	Определяются вузом с учётом рекомендаций УМО		

УМО (учебно-методическое объединение) в области ИБ создано на базе ИКСИ (институт криптографии, связи и информатики) Академии Федеральной службы безопасности

ФЕДЕРАЛЬНЫЙ ГОСУДАРСТВЕННЫЙ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (КВАЛИФИКАЦИЯ (СТЕПЕНЬ) "БАКАЛАВР«)

ФГОС ВПО

Представляет собой совокупность требований, обязательных при реализации основных образовательных программ бакалавриата по направлению подготовки 10.03.01 Информационная безопасность образовательными учреждениями высшего профессионального образования (высшими учебными заведениями, вузами), имеющими государственную аккредитацию, на территории Российской Федерации.

Право на реализацию основных образовательных программ высшее учебное заведение имеет только при наличии соответствующей лицензии, выданной уполномоченным федеральным органом исполнительной власти (ФСБ РФ)

1 ПРОГРАММЫ ВПО В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальности ВПО в области ИБ

Код специальности	Название	срок	квалиф
090301	***Компьютерная безопасность***	5	Специалист по ЗИ
090302	***Информационная безопасность телекоммуникационных систем***	5	Специалист по ЗИ
090303	***Информационная безопасность автоматизированных систем***	5	Специалист по ЗИ
090304		5	Специалист по ЗИ
090305	**Информационно-аналитические системы безопасности**	5	Специалист по ЗИ

2. СОЦИАЛЬНАЯ ЗНАЧИМОСТЬ ПРОФЕССИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ХАРАКТЕРИЗУЕТСЯ ВАЖНОЙ (ОГРОМНОЙ) ЗНАЧИМОСТЬЮ ОБЪЕКТОВ ЗАЩИТЫ

НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Составляющая

"НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ" - состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СУБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИБ: личность, общество, государство

ОБЪЕКТЫ (принадлежащие личности, обществу и государству):

1.ИНФОРМАЦИЯ : В РАЗЛИЧНЫХ ФОРМАХ В Т.Ч ИНФОРМАЦИОННЫЕ РЕСУРСЫ;

2. СИСТЕМЫ И СРЕДСТВА ОБРАБОТКИ ИНФОРМАЦИИ (СВТ, АС, ИС, ИТКС И др.)

3. ПОМЕЩЕНИЯ ДЛЯ ВЕДЕНИЯ ПРИВАТНЫХ ПЕРЕГОВОРОВ;

4. КРИТИЧЕСКИ ВАЖНЫЕ ОБЪЕКТЫ РАБОТАЮЩИЕ ПОД УПРАВЛЕНИЕМ АСУ

ОБЪЕКТЫ (принадлежащие личности, обществу и государству) в сферах внутриполитическая сфера; экономическая сфера; социальная сфера; сфера науки и образования; международная сфера; информационная сфера; экологическая сфера; военная сфера; сфера общественной безопасности; оборонно-промышленная сфера; духовная сфера.

Информация: **Государственная тайна, Персональные данные (банковская, налоговая, профессиональная тайна, коммерческая тайна**

3.ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ БАКАЛАВРОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».

КОНЦЕПЦИЯ ООП

Социальная роль (миссия) ООП ВПО заключается в подготовке бакалавров с уровнями их нравственного, физического и интеллектуального развития, обеспечивающими социальную готовность для жизни в современном быстро меняющемся и усложняющемся мире и профессиональную готовность реализовать свои компетенции в области информационной безопасности в соответствии с потребностями общества, государства, личности на предприятиях города, края, других субъектов Российской Федерации, а также продолжить обучение на втором уровне ВПО в магистратуре по соответствующему направлению подготовки

Цели ООП ВПО

Цель 1. Формирование способностей к самосовершенствованию и профессиональному росту с разносторонними гуманитарными и естественнонаучными знаниями и интересами.

Цель 2. Готовность выпускников к эксплуатации компонентов систем комплексной защиты объектов информатизации, администрированию подсистем информационной безопасности объекта (АС и ИТКС), участию в проведении аттестации объектов информатизации (в том числе помещений) по требованиям безопасности информации

Цель 3. Готовность выпускников к проектно- технологической деятельности, включая анализ исходных данных для проектирования систем, проведение проектных расчетов элементов систем обеспечения информационной безопасности, участие в разработке технологической и эксплуатационной документации;

Цель 4. Готовность выпускников к экспериментально - исследовательской деятельности, включающей сбор, изучение научно-технической информации, проведение экспериментов по заданной методике, обработка и анализ результатов, проведение вычислительных экспериментов с использованием стандартных программных средств

Цель 5. Готовность выпускников к организационно – управленческой деятельности, включая организацию работы малых коллективов исполнителей, организацию технологического процесса комплексной защиты информации объекта, разработку предложений по совершенствованию системы управления информационной безопасности

3.ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ БАКАЛАВРОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».

ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКА ООП ВПО НАПРАВЛЕНИЯ ПОДГОТОВКИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Область профессиональной деятельности выпускника

Область профессиональной деятельности бакалавра информационной безопасности включает: сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

Объекты профессиональной деятельности выпускника

Объектами профессиональной деятельности бакалавров являются:

- Объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии *в условиях существования угроз в информационной сфере;*

-технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;

- процессы управления информационной безопасностью защищаемых объектов.

Виды профессиональной деятельности выпускника

Бакалавр по направлению подготовки «Информационная безопасность», с учётом предложений научно-педагогических работников АлтГТУ и представителей работодателей, готовится к следующим видам профессиональной деятельности:

А) основные

эксплуатационная;

проектно-технологическая;

Б) не являются основными, а приобретённые базовые знания при их освоении способствуют расширению профессиональных и общекультурных компетенций

экспериментально-исследовательская;

организационно-управленческая.

3.ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ БАКАЛАВРОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».

ЗАДАЧИ К РЕШЕНИЮ КОТОРЫХ ГОТОВИТСЯ ВЫПУСКНИК

ВИДЫ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

ОСНОВНЫЕ

Не являются основными, а приобретённые базовые знания при их освоении способствуют расширению профессиональных и общекультурных компетенций

- **ЭКСПЛУАТАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ**
- **ПРОЕКТНО-ТЕХНОЛОГИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ**
- **ЭКСПЕРИМЕНТАЛЬНО-И СЛЕДОВАТЕЛЬСКАЯ ДЕЯТЕЛЬНОСТЬ**
- **ОРГАНИЗАЦИОННО-УПРАВЛЕНЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ**

ЗАДАЧИ В СООТВЕТСТВИИ С ВИДАМИ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ И ПРОФИЛЕМ ПОДГОТОВКИ

ЭКСПЛУАТАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ	ПРОЕКТНО-ТЕХНОЛОГИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ	ЭКСПЕРИМЕНТАЛЬНО-И СЛЕДОВАТЕЛЬСКАЯ ДЕЯТЕЛЬНОСТЬ	ОРГАНИЗАЦИОННО-УПРАВЛЕНЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ
- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований; - участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации; - администрирование подсистем информационной безопасности объекта	- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности; - проведение проектных расчетов элементов систем обеспечения информационной безопасности; - участие в разработке технологической и эксплуатационной документации; -проведение предварительного технико-экономического обоснования проектных расчетов	- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования; - проведение экспериментов по заданной методике, обработка и анализ результатов; - проведение вычислительных экспериментов с использованием стандартных программных средств	- осуществление организационно-правового обеспечения ИБ объекта защиты; - организация работы малых коллективов исполнителей с учетом требований защиты информации; - совершенствование системы управления ИБ; - изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны; - контроль эффективности реализации политики ИБ объекта.

3.ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ БАКАЛАВРОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».

УЧЕБНЫЙ ПЛАН

№ п/п	Наименование циклов и дисциплин	Распределение по семестрам			
		Экзамены	Зачеты	Курсовые про-екты (работы)	Расчетные задания
1	2	ЭКЗ	ЗАЧ	КП	РЗ
Б.1	**ГУМАНИТАРНЫЙ, СОЦИАЛЬНЫЙ И ЭКОНОМИЧЕСКИЙ ЦИКЛЫ**				
	Базовая часть				
1	История	1			
2	Философия	3			
3	Иностранный язык	4	123		
4	Экономика		4		
5	Правоведение		5		
6	Основы управленческой деятельности		5		
	Вариативная часть, включая дисциплины по выбору				
7	Социология		2		
8	Политология		4		
9	Английский язык для IT-специалистов		5		
	Дисциплины по выбору:				
10.1	Социально-психологические основы общения		2		
10.2	Мировая и отечественная культура		2		
	Английский язык в сфере				

Б.2	**МАТЕМАТИЧЕСКИЙ И ЕСТЕСТВЕННОНАУЧНЫЙ ЦИКЛ**				
	Базовая часть				
1	Математика	123			2
2	Теория вероятностей и математическая статистика		4		
3	Дискретная математика		2		2
4	Физика	4	3		4
5	Информатика	1			1
6	Теория информации		6		
	Вариативная часть, включая дисциплины по выбору				
7	Введение в математику		1		
8	Математическая логика и теория алгоритмов		4		4
9	Введение в физику	2			
10	Современная научная картина мира	6			
11	Информационные процессы и системы		2		
	Дисциплины по выбору:				
12.1	Основы теории чисел		3		
12.2	Основы вычислительной математики		3		
13.1	Пакеты прикладных математических программ		4		
13.2	Физические основы работы компонентов измерительных и управляющих систем		4		
	ИТОГО по МЕНЦ	7	9		5

3.ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ БАКАЛАВРОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».

УЧЕБНЫЙ ПЛАН

Б.3	ПРОФЕССИОНАЛЬНЫЙ ЦИКЛ				
	Базовая (общепрофессиональная) часть				
1	Основы информационной безопасности	2	1		
2	Аппаратные средства вычислительной техники	2			2
3	Программно-аппаратные средства защиты информации	6			6
4	Криптографические методы защиты информации		7	7р	
5	Организационное и правовое обеспечение ИБ	4	3	3р	4
6	Техническая защита информации	5			
7	Сети и системы передачи информации	5			5
8	Безопасность жизнедеятельности		1		
9	Языки программирования	1		1р	
10	Технологии и методы программирования	3			3
11	Управление ИБ		7		
12	Документоведение		1		
13	Электротехника	3			3
14	Электроника и схемотехника	4			
15	Информационные технологии	5			5
	Вариативная часть, включая дисциплины по выбору				
16	Вычислительные сети	7		7р	
17	Информационная безопасность предприятия (организации)	8		8р	
18	Международные и российские нормативные акты и стандарты по информационной безопасности	7	6		
19	Информационно-аналитическая деятельность по обеспечению комплексной безопасности		6		6
20	Инженерно-техническая защита информации		6	6р	
21	Проверка информационной защищенности на соответствие нормативным документам		7		7
22	Основы WEB-технологий	7	6		7
23	Технические средства охраны		5		
24	Системы управления базами данных	5		5р	
25	Информационная безопасность автоматизированных систем	7			
	Дисциплины по выбору				
26.1	Основы моделирования	8	7		
26.2	Цифровая обработка сигналов	8	7		
27.1	Безопасность вычислительных сетей и их администрирование	8	7		8
27.2	Микроконтроллеры и их применение в ИБ	8	7		8
28.1	Правовое обеспечение компьютерной безопасности		3		
28.2	Правовая охрана результатов интеллектуальной собственности		3		
29.1	Основы научных исследований		8		
29.2	Информационно-измерительные и управляющие системы		8		
30.1	Измерительная аппаратура анализа защищенности объектов и электрорадиоизмерения		6		
30.2	Компьютерная графика		6		
31,1	Системы видеоконтроля и контроля управления доступом		8		
31.2	Основы радиотехники		8		

3.ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ БАКАЛАВРОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».

Основные результаты обучения	**Составляющие результатов обучения** (общекультурные и профессиональные компетенции на основе которых формируется совокупный результат)
1	**2**
Р1	Способность анализировать и понимать мировоззренческие проблемы с научных позиций, самостоятельно осваивать культурные богатства, логически верно и аргументировано мыслить и правильно строить устную и письменную речь (ОК — 3,4,8,9)
Р2	Способность к самопознанию, к критической оценке своих достоинств и недостатков и самосовершенствованию, к высокой мотивации своей профессиональной и гражданской активности (ОК — 2,5,6,12)
Р3	Способность анализировать социально значимые проблемы и процессы и использовать на практике методы гуманитарных, социальных и экономических наук в различных видах социальной и профессиональной деятельности (ОК — 1,2,3,4,7)
Р4	Способность к профессиональной письменной и устной коммуникации на русском языке. Знание иностранного языка на уровне, необходимом для выполнения профессиональных задач (ОК — 9,10)
Р5	Способность использовать в профессиональной деятельности базовые знания математических дисциплин, обрабатывать и анализировать числовые данные, изучать характер зависимостей между различными величинами, на языке математики формулировать и решать задачи, возникающие в практической деятельности. (ОК 8, 9, 11, 12; ПК 1, 18, 20, 22)
Р6	Наличие целостного представления о современной научной картине мира. Способность использовать знание основных положений естественнонаучных дисциплин для понимания процессов и явлений природы, регулирования отношений человека и окружающей среды, для проведения простейших наблюдений и исследований, принятия решений, связанных с профессиональной деятельностью, организацией экспертиз, диагностики, контроля качества объектов и процессов.(ОК 8, 9, 11, 12; ПК 20, 22)
Р7	Владение основными методами и средствами получения, хранения, обработки и защиты экономической, научно-технической и другой информации, способность работать в глобальных и корпоративных компьютерных сетях, применять стандартные пакеты прикладных программ, адаптироваться к новым программным продуктам и новой компьютерной и информационной технике, вести информационное обслуживание производственной деятельности. (ОК 8, 9, 11, 12; ПК 2, 8, 9, 12, 14, 18, 19, 21, 23, 24)

3.ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ БАКАЛАВРОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».

Р8	Способность применять комплексный подход к обеспечению информационной безопасности, формировать и обеспечивать комплекс мер по информационной безопасности объекта защиты (объекта информатизации) при различных условиях внешних воздействий и вероятных угроз, организовать и сопровождать аттестацию объекта на соответствие требованиям нормативных документов (ПК-3,4,5, 6,30)
Р9	Способность устанавливать, настраивать, обслуживать, эксплуатировать технические и программно-аппаратные средства защиты информации и администрировать подсистемы информационной безопасности объекта (ПК-9,10,11)
Р10	Способность собрать и провести анализ данных для проектирования подсистем и средств обеспечения информационной безопасности, обосновать проектные решения, оформить рабочую и техническую документацию (ПК-,12,13,14,18)
Р11	Способность применять программные средства системного, прикладного и специального назначения для решения профессиональных задач и выполнять программную реализацию алгоритмов решения типовых задач обеспечения информационной безопасности (ПК15,16,17)
Р12	Способность проводить эксперименты по заданной методике и обработку их результатов, определять виды и возможные методы реализации угроз на основе анализа информационных процессов предприятия, анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-8, 20,21,22,23)
Р13	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составить обзор по вопросам обеспечения информационной безопасности (ПК -19,24)
Р14	Способностью формировать комплекс мер (правила, процедуры) и предложения по совершенствованию для управления информационной безопасностью (ПК -25,26,)
Р15	Способность принимать участие в организации контрольных проверок работоспособности средств защиты информации, в работах по реализации политики информационной безопасности, изучать и обобщать опыт других организаций по повышению эффективности защиты информации (ПК-27-29)
Р16	Способность организовать: а) работу малого коллектива исполнителей с учетом требований защиты информации; б) технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами (ПК-31,33)
Р17	Способность использовать основные методы защиты персонала от возможных последствий аварий, катастроф, стихийных бедствий и организовать мероприятия по охране труда в процессе использования средств защиты информации (ПК-7,-32)

3.ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ БАКАЛАВРОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».

Общекультурные и профессиональные компетенции в соответствии с ФГОС

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОСНОВНЫХ
ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ БАКАЛАВРИАТА

5.1. Выпускник должен обладать следующими общекультурными компетенциями (ОК):
способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма (ОК-1);
способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм (ОК-2);
способностью уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия (ОК-3);
способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач (ОК-4);
способностью к кооперации с коллегами, работе в коллективе (ОК-5);
способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-6);
способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-7);
способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления (ОК-8);
способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-9);
способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного (ОК-10);
способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства (ОК-11);
способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков (ОК-12);
способностью к самостоятельному применению методов физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, готовностью к достижению должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (ОК-13).
5.2. Выпускник должен обладать следующими профессиональными компетенциями (ПК):
общепрофессиональными:
способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1);
способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2);
способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3);
способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4);
способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-5);
способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6);
способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ПК-7);
способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-8);
эксплуатационная деятельность:
способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9);
способностью администрировать подсистемы информационной безопасности объекта (ПК-10);
способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-11);
проектно-технологическая деятельность:
способностью участвовать в разработке подсистемы управления информационной безопасностью (ПК-12);
способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности (ПК-13);
способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности (ПК-14);
способностью применять программные средства системного, прикладного и специального назначения (ПК-15);
способностью использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-16);
способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности (ПК-17);
способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-18);
экспериментально-исследовательская деятельность:
способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности (ПК-19);
способностью применять методы анализа изучаемых явлений, процессов и проектных решений (ПК-20);
способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-21);

4. ПРОГРАММА ДИСЦИПЛИНЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».

ОБЩИЕ СВЕДЕНИЯ О ДИСЦИПЛИНЕ. ПАСПОРТ ДИСЦИПЛИНЫ

Выписка из рабочего учебного плана ООП

Цикл - профессиональный цикл
Часть цикла - базовая (общепрофессиональная) часть
Курс обучения -1
Семестр – 1,2
Трудоёмкость - 5 ЗЕ
Учебных часов всего – 180,
1семестр- 68.
2 семестр - 112
Всего без СРС в период сессий-135
Аудиторные занятия -85
Лекции -51
Практические занятия -34
СРС- 95
В семестре -50
В период сессий -45
Перечень реализуемых компетенций ОК-7;9,11 ПК-2, ПК-3, ПК-19
Учебных занятий в интерактивной форме, час -34
Формы промежуточной аттестации 1 семестр –зачёт, 2 семестр-экзамен

Распределение по видам занятий

Семестр	Учебные занятия (час.)					Наличие (КП), (РЗ)	Форма итоговой аттестации
	Аудиторные				СРС		
	всего	лекции		ПЗ (семинары)			
1	34	17		17	34	-	Зач.
2	51	34		17	61	-	Экз.

4. ПРОГРАММА ДИСЦИПЛИНЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».

ОБЩИЕ СВЕДЕНИЯ О ДИСЦИПЛИНЕ. ПАСПОРТ ДИСЦИПЛИНЫ

Цели освоения дисциплины

усвоение теоретических знаний, практических умений и навыков в области основ информационной безопасности и защиты информации, овладение компетенциями по квалифицированному применению на практике профессиональной терминологии, по классификации защищаемой информации средств и систем её защиты, проведению целенаправленного поиска в различных источниках информации по основам информационной безопасности и защиты информации, в том числе в глобальных компьютерных системах.

Задачи освоения дисциплины

Достижение цели предполагает выполнение следующих задач:

- ознакомление с источниками информации в области профессиональной деятельности, в том числе с ресурсами в сети Интернет, со структурой комплексной системы защиты информации на предприятии, современными проблемами обеспечения информационной безопасности и защиты информации.

- изучение основных понятий и систем классификации в области информационной безопасности, таких как защищаемая информация, объекты защиты, угрозы безопасности информации и риски, политика безопасности, системы и средства обеспечения информационной безопасности и защиты информации;

- изучение состава объектов обеспечения информационной безопасности, угроз безопасности информации и объектам защиты, методов и средств защиты информации на объектах информатизации, общих принципов построения и функционирования систем обеспечения информационной безопасности;

- формирование первичных навыков по определению объектов защиты информации, определению угроз безопасности информации на этих объектах, определению необходимых классов защиты информации от НСД по требованиям безопасности информации для СВТ и АС.

4. ПРОГРАММА ДИСЦИПЛИНЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».

ОБЩИЕ СВЕДЕНИЯ О ДИСЦИПЛИНЕ. ПАСПОРТ ДИСЦИПЛИНЫ

Место дисциплины в структуре ООП направления

Дисциплина входит в базовую часть профессионального цикла образовательной программы бакалавра (Б3).

Дисциплина является вводной в проблематику информационной безопасности, поэтому студент должен иметь начальные сведения по математике, информатике и физике в объеме школьного курса.

Дисциплина является предшествующей и необходимой для изучения таких дисциплин (корреквизитов) как:

- «Организационно-правовое обеспечение информационной безопасности» (3,4 семестры),
- «Программно-аппаратные средства защиты информации» (6 семестр),
- «Техническая защита информации» (6 семестр),
- «Криптографические методы защиты информации» (7 семестр).
- «Управление информационной безопасностью» (7 семестр),
- «Информационно-аналитическая деятельность по обеспечению комплексной безопасности» (6 семестр),
- «Информационная безопасность автоматизированных систем» (7 семестр)
-«Информационная безопасность предприятия (организации)» (8 семестр).

4. ПРОГРАММА ДИСЦИПЛИНЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

а) основная литература:

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. Алт.гос.техн.ун-т им.И.И.Ползунова.- Баранаул: -2011-253с. (60 экз.Гриф УМО)

2.Расторгуев С.П. Основы информационной безопасности. .- М.: Издательский центр «Академия», 2008.- 192с. (20экз. Гриф УМО)

3.Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций. - Барнаул: АлтГТУ, 2010 –*[электронный ресурс]:-* / *режим доступа: 1*. Ауд.98. D, Загинайлов, ТИБМЗИ, 2.http://www.elib.altstu.ru

б) дополнительная литература:

4.Мельников В. П. Информационная безопасность и защита информации: учебное пособие для студ. высш. учеб. заведений / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под. ред. С. А. Клейменова. — 3-е изд., стер. - М.: Издательский центр «Академия», 2008. — 336 с. (20экз.-Гриф УМО.)

5.Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб.пособие для вузов.-М:Горячая линия-Телеком, 2004.-280с. (15экз.библ- гриф МО. РФ).

в) программное обеспечение и Интернет-ресурсы:

При проведении семинаров и самостоятельной работе студентов используется информационные ресурсы включающий в себя:

6.Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России *[электронный ресурс]:- режим доступа:* http:// www.fstec.ru.

7.Официальный сайт федерального агентства по техническому регулированию и метрологии [электронный ресурс]: режим доступа: http://protect.gost.ru//

8.Правовая справочная система «Гарант» *[электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ*.(Платформа F1 Гарант)*; 2. http://www.garant.ru*

г) учебно-методические материалы и пособия для студентов, используемые при изучении дисциплины:

9.Загинайлов Ю.Н. Методические рекомендации к семинарским (практическим) занятиям и указания к СРС по дисциплине «Основы информационной безопасности»/ Алт.гос.техн.ун-т им.И.И.Ползунова.- 2011- 92с. *[электронный ресурс]: -режим доступа: 1*. Ауд.98. D, Загинайлов, ОИБ, 2.http://www.elib.altstu.ru

10. Загинайлов Ю.Н. Информационная безопасность в терминах и определениях законодательства и стандартов защиты информации: учебно-справочное пособие /Ю.Н.Загинайлов, Е.В. Урминский.- Алт. гос. тех. ун-т им. И.И. Ползунова. – Барнаул, 2010. - 204с. *[электронный ресурс]: -режим доступа: 1*. Ауд.98. D, Загинайлов, ИБ термины, 2.http://www.elib.altstu.ru

4. ПРОГРАММА ДИСЦИПЛИНЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Перечень источников в области профессиональной деятельности, для формирования ПК *проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2), способности использовать нормативные правовые документы в своей профессиональной деятельности(ПК-3) включает:*

1.Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» *[электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/*

2.Закон РФ № 54-1 от 21.07.1993 г. «О государственной тайне». *[электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/*

3.Федеральный Закон РФ от 29.07.2004г. №98-ФЗ «О коммерческой тайне». *[электронный ресурс]: -режим доступа: http://www.garant.ru/*

4.Федеральный закон РФ № 152 –ФЗ 2006г. «О персональных данных». *[электронный ресурс]: -режим доступа: http://www.garant.ru/*

5.ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения. М.: Стандартинформ, 2008 -10с. *[электронный ресурс]:- режим доступа:* http:// www.fstec.ru

6.ГОСТ Р 51275-2006. Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: Стандартинформ, 2007 -7с. *[электронный ресурс]:- режим доступа:* http:// www.fstec.ru.

7.ГОСТ Р ИСО/МЭК 13335-1-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телеком-уникационных технологий. М.: Стандартинформ, 2007 -19с.

8.Руководящий документ. Средства вычислительной техники Защита от несанкционированного доступа к информации. Показатели защищенности от несанк-ционированного доступа к информации *[электронный ресурс] : -режим доступа:* http://www.fstec.ru/_razd/_isp0o.htm- Загл. с экрана.

9.Руководящий документ. Автоматизированные системы. Защита от несан-кционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации *[электронный ресурс] : -режим доступа:* http://www.fstec.ru/_razd/_isp0o.htm- Загл. с экрана.

10.Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации *[электронный ресурс] : -режим доступа* http://www.fstec.ru/_razd/_isp0o.htm- Загл. с экрана.

11.Руководящий документ. Антивирусные средства. Показатели защищенности и требования по защите от вирусов. РД ГТК. РФ. Средства антивирусной защиты. Показатели защищенности и требования по защите от вирусов. Показатели защищенности от вирусов. - М. 1997.

12.Указ Президента Российской федерации от 06.03.97 № 188 "Об утверждении перечня сведений конфиденциального характера" *[электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ*.(Платформа F1 Гарант);

13.Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895). *[электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/*

14.Стратегия национальной безопасности Российской Федерации. *[электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/*

15.Стратегия построения информационного общества в Российской Федерации. *[электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/*

16.Федеральный закон Российской Федерации от 12.10 «О безопасности» *[электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/*

17.Руководящий Документ (ГОСТ Р 15408)

4. ПРОГРАММА ДИСЦИПЛИНЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».

САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Распределение нагрузки СРС по видам и семестрам приведено в таблице

Вид СРС	1 сем, час	2сем, час	Всего, час	Литература
Подготовка к лекционным занятиям	0,5x8=4	0,25x16=4	12	[3]
Подготовка к практическим занятиям	1,5x8=12	1,0x8=8	24	[9,10]
Написание реферата	1,0x8=8	18 (в период сессии)	16	[1-10]
Подготовка к письменным контрольным опросам	2x3=6	1,33x3=4	12	[1,3]
Подготовка к зачёту	4	-	4	[1-10]
Подготовка к экзамену	-	45	27	[1-10]
Всего	34	61	95	

Рекомендуется следующий сценарий изучения каждой темы дисциплины:

- ознакомление с материалом предстоящей по плану темой лекции – путём просмотра курса визуальных лекций (Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: курс визуальных лекций. - Барнаул: АлтГТУ, 2010 –*[электронный ресурс]:-* / *режим доступа: 1*. Ауд.98. D, Загинайлов, ТИБМЗИ, 2.http://www.elib.altstu.ru [3]);
- заучивание терминов и их определений из базового перечня к данной теме наизусть [9];
- конспектирование материалов в конспект (рабочую тетрадь) в период чтения лекции преподавателем [3];
- повторение материала лекции и углубление знаний по рассматриваемым вопросам при подготовке к практическому или семинарскому занятию с использованием основного пособия [1]);:
- изучение вопроса темы заданного на самостоятельное изучение, конспектирование материала [1]);
- работа по теме реферата [1-10, 1-17 п.4.2.1]);;
- самоконтроль знания терминов и их определений из базового перечня к данной теме, при необходимости «доучивание» их до знания наизусть;
- изучение и сравнение иных подходов к рассмотрению изучаемых вопросов темы в «альтернативном» изложении в других учебных пособиях, приведенных в списке основной литературы [4-6];

4. ПРОГРАММА ДИСЦИПЛИНЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».

САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Основные темы рефератов

Информационная безопасность личности в «информационном обществе»;
Информационная война и информационное оружие.
Система угроз информационной безопасности Российской Федерации.
Органы обеспечения информационной безопасности в Российской Федерации, их функции и задачи.
Свойства информации как объекта защиты.
Носители информации и системы их классификации;
Объекты интеллектуальной собственности в составе защищаемой информации;
Концепции защиты информации.
Модели систем и процессов защиты информации.
Персональные данные как информация ограниченного доступа.
Служебная тайна как информация ограниченного доступа.
Профессиональная тайна как информация ограниченного доступа
Современные системы классификации угроз безопасности защищаемой информации.
Виды и способы реализации угроз безопасности информации.
Уязвимости систем обработки информации
Классификация и характеристика технических каналов утечки информации.
Криптоанализ как метод НСД к защищаемой информации.
Современные методы несанкционированного доступа к конфиденциальной информации в автоматизированных системах;
Направления, виды и особенности деятельности иностранных спецслужб по несанкционированному доступу к защищаемой информации (по отдельным странам);
Средства и системы обработки информации как объекты защиты.
Современные криптографические средства защиты информации;
Современные программно-аппаратные средства защиты информации (на примере сертиф-х средств)
Требования к системам защиты автоматизированных систем.
Стандартизация в области информационной безопасности и защиты информации в Российской Федерации.
Классификация средств вычислительной техники по уровню защищённости от НСД.
Классификация автоматизированных систем и требования по защите информации.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №1

ПЛАН ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ ПО ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ БАКАЛАВРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Цели ПЗ:

1. *Разработка студентом индивидуального обобщённого плана формирования компетенций по образовательной программе бакалавра направления подготовки «Информационная безопасность».*
2. *Формирование первичных умений анализа нормативных документов с интересах своей учебной и профессиональной деятельности.*

Практическое задание

Составить план формирования компетенций по образовательной программе, используя рабочий учебный план, концепцию ООП 10.03.01 АлтГТУ, ГОС ВПО 10.03.01 Информационная безопасность.

Результатом работы должен быть посеместровый график прохождения дисциплин с видом аттестации, цели и результаты освоения ООП, перечень компетенций в соответствии с ГОС ВПО 10.03.01 Информационная безопасность, выполненный в рабочей тетради.

Порядок выполнения задания

1.Составить посеместровый график изучения учебных дисциплин используя рабочий учебный план направления подготовки 10.03.01 в АлтГТУ. Номера семестров и вид аттестации по дисциплине (экзамен, зачёт) приводятся в первой и второй колонках соответственно, после наименования дисциплины.
2.Выписать в виде таблицы из Концепции ООП 10.03.01 АлтГТУ цели ООП и определить их как личные цели освоения ООП в период обучения в АлтГТУ.
3.Оформить в виде таблицы результаты освоения ООП и соответствующие им номера универсальных (ОК) и профессиональных (ПК) компетенций.
4.Используя ГОС ВПО 10.03.01 Информационная безопасность выписать соответствующие номерам ОК и ПК наименование (содержание) компетенций.
5. Представить план преподавателю для проверки.

Литература

ГОС ВПО 10.03.01 Информационная безопасность,
Рабочий учебный план направления подготовки 10.03.01,
Концепция ООП 10.03.01 АлтГТУ.

Контрольные вопросы (1 уровень)

1. Какие существуют программы подготовки по профессиям в области информационной безопасности (бакалавриаты, магистратуры, специалитеты) и на основе чего они разрабатываются.
2. Объясните и социальную значимость профессий в области информационной безопасности.
3. Каковы цели основной образовательной программы по направлению подготовки бакалавров «Информационная безопасность».
4. Приведите кратко тематический план дисциплины «Основы информационной безопасности».

Контрольные вопросы (2 уровень)

1.Каковы результаты основной образовательной программы по направлению подготовки бакалавров «Информационная безопасность».

Методические рекомендации по подготовке к занятиям

1.

(раздаточный материал:
ГОС ВПО 10.03.01 Информационная безопасность,
рабочий учебный план направления подготовки 10.03.01,
концепция ООП 10.03.01 АлтГТУ)