Министерство образования и науки Российской Федерации

ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ И ПРАВА» В Г. УСТЬ-ИЛИМСКЕ
(Филиал ФГБОУ ВПО «БГУЭП» в г. Усть-Илимске)

УТВЕРЖДАЮ
Директор
А.В. Бандурист

ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ Б.2.ДВ.1

Направление подготовки: 38.03.01 Экономика
Квалификация (степень) выпускника *Бакалавр*
Форма обучения Очная

Курс	3
Семестр	5
Лекции	17
Практические (семинарские, лабораторные) занятия	55
Самостоятельная работа	144
Всего часов	216
Зачет (семестр)	
Экзамен (семестр)	5

Усть-Илимск 2011

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Защита информации» является:

- формирование знаний и умений, связанных с организацией информационной безопасности, планированием, подготовкой и реализацией процесса информационной безопасности, освоение различных технологий обеспечения информационной безопасности, применение форм и методов обучения с учетом возрастных особенностей и специфики обучения.

Задачи:

- получение знаний о современных средствах, методах и технологиях обеспечения информационной безопасности ВС/ИС;
- получение навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах;
- приобретение практических навыков организации работ по обеспечению информационной безопасности на предприятиях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП БАКАЛАВРИАТА

Дисциплина «Защита информации» базируется на циклах Б.1 и Б.2 в базовой и вариативной частях. Дополняет другие дисциплины общеобразовательного цикла и предназначена для подготовки студентов к трудовой деятельности.

Данная дисциплина дает базовую основу для понимания, анализа и оценки основных проблем, связанных с обеспечением информационной безопасности предприятия и защитой информации, а также разработкой, внедрением и сопровождением средств информационной защиты, и их изучение базируется на полученных студентами знаниях при освоении предшествующих дисциплин «Математический анализ», «Информационные технологии в экономике».

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В совокупности с другими дисциплинами базовой части ФГОС ВПО дисциплина «Защита информации» направлена на формирование следующих общекультурных (ОК) и профессиональных (ПК) компетенций бакалавра по направлению подготовки 38.03.01 Экономика.

Компетентностная карта дисциплины

Код компетенции	Компетенция
ОК-12	способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны
ОК-13	владеет основными методами, способами и средствами пополнения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией, способен работать с информацией в глобальных компьютерных сетях.
ПК-12	способен использовать для решения коммуникативных задач современные технические средства и информационные технологии.

Ключевыми компетенциями, формируемыми в процессе изучения дисциплины являются ОК-12, ОК-13.

Уровневое описание признаков компетенции ОК-12:
способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны.

Уровень освоения	Признаки проявления
Продвинутый (91 – 100 баллов)	базовый уровень и умение выявлять достоинства и недостатки разных архитектур информационной безопасности, умение находить решения, соответствующие требованиям наилучшим образом, выражая обоснованные предположения о возможных угрозах после применения выбранного средства защиты, на основе мировой практики использования конкретного метода и статистики последующих угроз.
Базовый (71 – 90 баллов)	минимальный уровень и умение решать задачи различными методами, понимание преимуществ и недостатков каждого решения, оценка ресурсов, обеспечивающих каждое решение, обоснование выбранных средств защиты.
Минимальный (41 – 70 баллов)	знать основные структуры хранения информации и программно-технические средства, применяемые в целях защиты, уметь применять средства криптографии и кодирования используя встроенные средства защиты, знать технологию взаимодействия клиентских программ и серверов методов их протоколирования, способы распределения функций защиты между клиентскими приложениями и серверами.

Уровневое описание признаков компетенции ОК-13:
владеет основными методами, способами и средствами пополнения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией, способен работать с информацией в глобальных компьютерных сетях.

Уровень освоения	Признаки проявления
Продвинутый (91 – 100 баллов)	базовый уровень и умение выявлять достоинства и недостатки статей ГК РФ относящихся к сфере защиты информации, выражать предположение о внесении поправок с обоснованием и доказательством в виде судебных прецедентов встречающихся в Российской и международной судебных практиках, умение находить решения, наилучшим образом соответствующие требованиям.
Базовый (71 – 90 баллов)	минимальный уровень и умение решать задачи различными методами, понимание преимуществ и недостатков каждого решения, оценка достаточности правовых ресурсов содержащихся в ГК РФ, обеспечивающих решения.
Минимальный (41 – 70 баллов)	иметь представление методах, способах и средствах пополнения, хранения, переработки информации о содержании статей ГК РФ, уметь квалифицировать преступления совершенные в сфере информационный технологий, уметь отражать меры ответственности граждан умышленно совершивших противоправное действие, уметь создавать средства защиты классифицируя их и обосновывая выбор конкретного программного или аппаратного продукта, применять средства администрирования и мониторинга в целях обеспечения информационной безопасности.

В результате освоения дисциплины «Защита информации» обучающийся должен:

Знать:

– современную научную парадигму защиты информации;

– организационно-правовые основы защиты информационных ресурсов предприятия;

– теоретические и практические знания по правовым основам защиты информации при работе на вычислительной технике и в каналах связи;

– модели, стратегии, систем и технологических основ комплексного обеспечения защиты информации;

– вопросы правового и организационного обеспечения защиты информации;

– о концепции защиты информации;

– содержание основных понятий обеспечения защиты информации;

– источники угроз безопасности информации;

– методы оценки уязвимости информации;

– методы создания, организации и обеспечения функционирования систем комплексной защиты информации;

– методы пресечения разглашения конфиденциальной информации;

– виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений.

Уметь:

– решать вопросы в сфере обеспечения защиты информации;

– применить практические навыки и способности по осуществлению мероприятий по обеспечению защиты информации компьютерных сетей;

– использовать методы и средства защиты данных;

– выполнять анализ способов нарушений информационной безопасности;

– отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;

– применять действующую законодательную базу в области защиты информации;

– разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

Владеть:

– криптографическими, программно-аппаратными и техническими методами и средствами защиты информации;

– методами криптографической защиты;

– основными технологиями построения защищенных ЭИС;

– основными понятиями защиты информации;

– средствами обеспечения защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 6 зачетных единиц 216 часов.

4.1. Содержание разделов дисциплины

№ п/п	Раздел и тема дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Формы текущего контроля успеваемости
			Лекции	Семинар Практич.	Самост. раб.	
1	Обеспечение защиты информации: содержание и структура понятия.	5	3	8	26	Письменные работы, устные опросы
2	Стандарты и спецификации в области защиты информации	5	3	10	28	Письменные работы, устные опросы
3.	Комплексная система защиты информации	5	3	10	20	Письменные работы, устные опросы
4.	Процедурный уровень защиты информации.	5	5	15	37	Письменные работы, устные опросы
5	Административный уровень защиты информации	5	3	12	33	Письменные работы, устные опросы
	ИТОГО		17	55	144	

4.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1	Обеспечение защиты информации: содержание и структура понятия.	Проблемы защиты информации. Основы теории защиты информации. Системы защиты информации.
2	Стандарты и спецификации в области защиты информации	Роль стандартов и спецификаций в обеспечении защиты информации. Угрозы и методология оценки уязвимости информации.
3	Комплексная система защиты информации	Средства защиты информации. Системы защиты информации. Защита информации в персональных ЭВМ. Защита информации в сетях ЭВМ. Организация и обеспечение работ по защите информации. Обеспечение защиты информации в общемировых сетях.
4	Процедурный уровень защиты информации.	Характеристики защиты информации для различных информационных объектов. Методы определения требований к защите информации.

5	Административный уровень защиты информации	Политика информационной безопасности предприятия.

4.3. Семинарские, практические, лабораторные занятия, их содержание.

№ раздела и темы	Содержание и формы проведения
Раздел 1	*Проблемы защиты информации.* Цель и задачи курса. Понятие угрозы безопасности информации и общие подходы к ее классификации. Классификация угроз безопасности информации по способам их возможного негативного воздействия. Нарушители безопасности информации. Происхождение угроз безопасности информации. Предпосылки появления угроз *Контрольные вопросы* Цель и задачи курса. Понятие защиты информации. Важность и сложность проблемы защиты информации. Сервисные службы защиты. Нарушения. *Основы теории защиты информации.* Сущность теории защиты информации, ее основные составляющие и задачи. Моделирование процессов защиты информации. Стратегии защиты информации. *Контрольные вопросы* Механизмы защиты. Абстрактные модели защиты информации. Модели защиты сети. Модели защиты доступа к сети. Наиболее распространенные угрозы доступности. Некоторые примеры угроз доступности. *Системы защиты информации* Понятие и структура систем защиты информации. Типизация и стандартизация систем защиты информации. *Контрольные вопросы* Основные определения и критерии классификации угроз. Действия, приводящие к неправомерному овладении конфиденциальной информацией: разглашение. Действия, приводящие к неправомерному овладении конфиденциальной информацией: утечка. Действия, приводящие к неправомерному овладении конфиденциальной информацией: несанкционированный доступ. Вредоносное программное обеспечение. Основные угрозы целостности. Основные угрозы конфиденциальности. Основные принципы информационной безопасности. Основные задачи в сфере обеспечения защиты информации.

Раздел 2	*Роль стандартов и спецификаций в обеспечении защиты информации* Стандарты и спецификации в области защиты информации и их классификация. Общие сведения о стандартах и спецификациях в области защиты информации. *«Оранжевая книга». Гармонизированные критерии Европейских стран. Руководящие документы (РД) Гостехкомиссии России. X.800 «Архитектура безопасности для взаимодействия открытых систем». Спецификация Internet-сообщества RFC 1510 «Сетевой сервис аутентификации Kerberos (V5)». FIPS 140-2 «Требования безопасности для криптографических модулей». «Обобщенный прикладной программный интерфейс службы безопасности». Технические спецификации IPsec [IPsec]. TLS. X.500 «Служба директорий: обзор концепций, моделей и сервисов». Рекомендация Internet-сообщества «Руководство по информационной безопасности предприятия». Рекомендация «Как выбирать поставщика Internet-услуг». Британский стандарт BS 7799 «Управление информационной безопасностью. Практические правила».* *Контрольные вопросы* Функции государственной системы по обеспечению информационной безопасности. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт. Информационная безопасность распределенных систем. Рекомендации X.800. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий". Гармонизированные критерии Европейских стран. Интерпретация "Оранжевой книги" для сетевых конфигураций. Руководящие документы Гостехкомиссии России. *Угрозы и методология оценки уязвимости информации.* Определение и содержание понятия угрозы информации в современных системах ее обработки. Возможные подходы к формированию множества угроз информации. Цели и задачи оценки угроз информации. Классификация и содержание угроз информации. Методы и модели оценки уязвимости информации. *Контрольные вопросы* Административный уровень защиты информации. Политика безопасности. Программа безопасности. Процедурный уровень защиты информации. Основные классы мер процедурного уровня. Управление персоналом.

Раздел 3	*Средства защиты информации.* Технические средства защиты. Программные средства защиты. Организационно-правовые средства защиты. Криптографические средства защиты. *Контрольные вопросы* Перечень технических средств защиты. Перечень программных средств защиты. Характеристика организационно-правовых средств защиты. Основные аспекты криптографии. Основные аспекты криптоанализа. Модели криптографии К. Шеннона. Теоретико-информационные оценки стойкости симметричных криптосистем. Потоковые шифры. Блочные шифры. *Системы защиты информации.* Основы архитектурного построения систем защиты. Типизация и стандартизация систем защиты. Методы проектирования систем защиты. Управление функционированием систем защиты. *Контрольные вопросы* Основы архитектурного построения систем защиты. Типизация и стандартизация систем защиты. Характеристика методов проектирования систем защиты. Анализ управления функционированием систем защиты. *Защита информации в персональных ЭВМ.* Угрозы информации в ПЭВМ. Обеспечение целостности информации в ПЭВМ. Защита ПЭВМ от несанкционированного доступа. Защита информации от копирования. Защита информации от вредоносных закладок. *Контрольные вопросы* Оценка угрозы целостности информации в ПЭВМ. Механизмы обеспечения целостности информации в ПЭВМ. Способы защиты ПЭВМ от несанкционированного доступа. Способы защиты информации от копирования. Правила защиты информации от вредоносных закладок. *Защита информации в сетях ЭВМ.* Архитектура механизмов защиты информации в сетях ЭВМ. Пример системы защиты ЛВС. *Организация и обеспечение работ по защите информации.* Основные вопросы организации и обеспечения работ по защите информации. Структура и функции органов защиты информации. Документационное обеспечение работ по защите информации. *Контрольные вопросы* Перечень основных организационных работ по защите информации. Структура и функции органов защиты информации. Список документационного обеспечения работ по защите информации. *Обеспечение защиты информации в общемировых сетях* Спецификации Internet-сообщества IPsec. *Архитектура средств безопасности IP-уровня. Контексты безопасности и управление ключами. Обеспечение аутентичности IP-пакетов. Обеспечение конфиденциальности сетевого трафика*. Роль поставщика Internet-услуг в реагировании на нарушения безопасности. Меры по защите Internet-сообщества. *Обеспечение безопасности маршрутизаторов. Особенности использования управляющих протоколов. Безопасное размещение сетевого оборудования потребителя. Защита системной инфраструктуры. Работа с Web-серверами.* *Контрольные вопросы* Описание архитектуры средств безопасности IP-уровня. Контексты безопасности и управление ключами. Обеспечение аутентичности IP-пакетов. Механизмы обеспечения конфиденциальности сетевого трафика. Инструменты обеспечения безопасности маршрутизаторов. Особенности использования управляющих протоколов. Безопасное размещение сетевого оборудования потребителя. Защита системной инфраструктуры.

Раздел 4	*Характеристики безопасности для различных информационных объектов* Операционные системы. Системы управления базами данных. Виртуальные частные сети. Виртуальные локальные сети. *Контрольные вопросы* Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ. Основные понятия программно-технического уровня защиты информации *Методы определения требований к защите информации.* Задача определения требований к защите информации. Существующие методики определения требований к защите информации. Факторы, влияющие на требуемый уровень защиты информации *Контрольные вопросы* Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.
Раздел 5	*Политика безопасности предприятия*. Нормы, правила и методики обращения, хранения и распределения информации. Номенклатура и содержание основных документов, обеспечивающих политику безопасности. *Контрольные вопросы* Направления обеспечения информационной безопасности. Законодательный уровень защиты информации. Правовые акты общего назначения, затрагивающие вопросы защиты информации. Закон "Об информации, информатизации и защите информации". Другие законы и нормативные акты.

4.4. Вид и форма промежуточной аттестации

Промежуточный контроль проводится в виде устного экзамена или итогового теста (по всему курсу, включая темы, изученные самостоятельно) в 5 семестре 3 курса.

5. ИСПОЛЬЗУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Реализация компетентностного подхода, в соответствии с требованиями ФГОС ВПО по направлению подготовки 38.03.01 Экономика, предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий: обсуждения поставленных проблем, групповых дискуссий, обсуждения результатов работы студенческих исследовательских групп. В сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Используются лекции с проблемным изложением, лекции-дискуссии, деловая игра, написание рефератов, метод проектов, обсуждение конкретных ситуаций, кейсы.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины «защита информации».

Доля занятий с использованием активных и интерактивных методов составляет не менее 50% аудиторных занятий (определяется требованиями ФГОС с учетом специфики ООП).

Занятия лекционного типа для соответствующих групп студентов составляют 33% аудиторных занятий (определяется требованиями ФГОС с учетом специфики ООП).

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

6.1. Текущий контроль

Текущий контроль осуществляется в соответствии с разработанной рейтинговой системе по дисциплине:

Контрольные мероприятия по дисциплине	Возможное количество балов	
	Минимум	Максимум
1. Выполнение и защита лабораторной работы Создание полного перечня потенциально возможных угроз информации предприятия с определением их количественных оценок и выбором средств защиты.	5	10
2. Выполнение и защита лабораторной работы Создание документа, определяющего цели, задачи и приоритеты системы безопасности предприятия. Определение номенклатуры документов, обеспечивающих политику безопасности предприятия.	5	10
3. Тестовый контроль.	5	10
4. Выполнение и защита лабораторных работ: Построение общей архитектуры системы безопасности предприятия. Определение состава средств и механизмов защиты и обоснование области их действия. Оценка гарантированного уровня защиты при проектировании системы защиты информации предприятия.	5	10
5. Написание реферата по дисциплине	10	10
6. Доклад на деловой игре (задание выдается индивидуально)	10	20
7. Зачет	10	20
Итого	50	100

6.2. Образцы тестовых и контрольных заданий текущего контроля

Пример теста к Разделу 2.

Укажите основные свойства VPN:

- Создает туннель, т.е. защищённый канал передачи данных
- Использует шифрование данных
- Реализуется в незащищенных или слабо защищенных сетях

Каковы функциональные возможности программы Retina WiFi Scanner:

- Вычисляет WEP-ключи методом brute force
- Генерирует отчёты
- Обнаруживает IP-адреса и другую сетевую информацию
- Обнаруживает неавторизованные беспроводные устройства

64- и 128-битное WEP-шифрование трафика на основе RC4 обеспечивает уровень безопасности

- Высокий
-Хороший
-Обычный
-Быстрый
- Оптимальный

Отметьте потенциально опасные с точки зрения утечек внутренней информации действия:

Размещение серверов в стороннем дата-центре

Хранение носителей вне офиса

Сервисный ремонт серверов или жестких дисков

Перевозка компьютеров или носителей

Какие режимы работы имеет программа Iris:

- Decode
- Capture

Используется ли VPN для защиты беспроводных сетей

-да
- нет
-редко
-часто

Сколько root key содержит реестр Windows

-5
-6
-3
-7

Какие решения применяются для контроля доступа к внешним устройствам:

- Secret Disk
- ZLock
- DeviceLock

Компьютер проверяет 10 млн. паролей в секудну. Сколько примерно времени ему потребуется, чтобы проверить методом словарной атаки все пароли для языка, содержащего 1 млн. слов:

- 0,1 секунды
- 0,5 секунды

- 0,8 секунды
- 0,9 секунды

Каково количество популярных паролей, которые остаются неизменными в течение последних 15 лет

- 500
- 300
- 250
- 400

Что позволяет выполнять программа Process Monitor:

- Отслеживать сетевую активность процесса
- Отслеживать обращение процесса к реестру
- Отслеживать работу процесса с файлами

Используется ли VPN для связи мобильного сотрудника с корпоративной сетью

- Да
- Нет

Можно ли применить заплатку реестра в командной строке:

- Да
- Нет

Интегрировано ли решение DeviceLock с Active Directory

- Да
- Нет

Позволяет ли DeviceLock контролировать FireWire-порты

- Да
- Нет

Используется ли VPN для обеспечения выхода в Интернет по защищенному каналу:

- Да
- Нет

Используется ли VPN для компьютерных игр через интернет

- Да
-Нет

Компьютер проверяет 10 млн. паролей в секудну. Сколько примерно времени ему потребуется, чтобы проверить методом Brute Force все 8-значные пароли для 120-символьного алфавита

- 100 лет
- 50 лет
- 30 лет
- 15 лет

Возможно ли отключить автозапуск autorun.inf внешних носителей через групповую политику:

- Да
- Нет

Укажите основные каналы утечек внутренней информации

- ноутбуки и КПК,

- физический доступ к оборудованию и носителям,
- интернет-службы,
- WiFi,
- мобильные носители информации

Примерная тематика вопросов к зачету (экзамену):

1. Понятие защиты информации.
2. Важность и сложность проблемы защиты информации.
3. Сервисные службы защиты
4. Нарушения
5. Механизмы защиты
6. Абстрактные модели защиты информации
7. Модели защиты сети
8. Модели защиты доступа к сети
9. Основные определения и критерии классификации угроз
10. Действия, приводящие к неправомерному овладении конфиденциальной информацией: разглашение
11. Действия, приводящие к неправомерному овладении конфиденциальной информацией: утечка
12. Действия, приводящие к неправомерному овладении конфиденциальной информацией: несанкционированный доступ
13. Наиболее распространенные угрозы доступности
14. Некоторые примеры угроз доступности
15. Вредоносное программное обеспечение
16. Основные угрозы целостности
17. Основные угрозы конфиденциальности
18. Основные принципы защиты информации
19. Основные задачи в сфере обеспечения защиты информации.
20. Функции государственной системы по обеспечению защиты информации.
21. Направления обеспечения защиты информации.
22. Законодательный уровень защиты информации.
23. Правовые акты общего назначения, затрагивающие вопросы защиты информации.
24. Закон "Об информации, информатизации и защите информации"
25. Другие законы и нормативные акты
26. Административный уровень защиты информации.
27. Политика безопасности
28. Программа безопасности
29. Процедурный уровень защиты информации
30. Основные классы мер процедурного уровня
31. Управление персоналом
32. Физическая защита
33. Поддержание работоспособности
34. Реагирование на нарушения режима безопасности

35. Планирование восстановительных работ

36. Основные понятия программно-технического уровня защиты информации.

37. Особенности современных информационных систем, существенные с точки зрения безопасности

38. Архитектурная безопасность

39. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт

40. Информационная безопасность распределенных систем. Рекомендации X.800

41. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

42. Гармонизированные критерии Европейских стран

43. Интерпретация "Оранжевой книги" для сетевых конфигураций

44. Руководящие документы Гостехкомиссии России

45. Основные аспекты криптографии

46. Основные аспекты криптоанализа

47. Модели криптографии К. Шеннона

48. Теоретико-информационные оценки стойкости симметричных криптосистем

49. Потоковые шифры

50. Блочные шифры

6.3. Тематика рефератов, эссе, докладов

1. Идентификация
2. Аутентификация
3. Целостность
4. Невозможность отречения
5. Управление доступом
6. Доступность
7. Конфиденциальность
8. Авторизация
9. Лицензирование и сертифицирование
10. Экранирование
11. Анализ защищенности
12. Протоколирование и аудит
13. Обеспечение высокой доступности (обеспечение отказоустойчивости, обеспечение безопастного и быстрого восстановления после отказов)
14. Туннелирование
15. Шифрование
16. Управление (мониторинг компонентов, контроль, координация работы компонентов системы)
17. Причины ослабления средств защиты

18. Утечка информации по техническим каналам связи
19. Конфиденциальность при работе с зарубежными партнерами
20. Стандарт X.509
21. Рекомендации IETF
22. Стандарт ISO/IEC 7498-2
23. Анализ антивирусного ПО
24. Сравнение ОС по качеству обеспечения ИБ
25. Защита беспроводных ЛВС

6.4. Темы курсовых работ, критерии оценивания

Курсовая работа не предусмотрена.

6.5. Методические указания по организации самостоятельной работы

Самостоятельная работа заключается:

- в самостоятельной подготовке студента к лекции – чтение конспекта предыдущей лекции. Это помогает лучше понять материал новой лекции, опираясь на предшествующие знания. В начале лекции проводится устный или письменный экспресс-опрос студентов по содержанию предыдущей лекции;
- в подготовке к практическим занятиям по основным и дополнительным источникам литературы;
- в выполнении домашних заданий;
- в самостоятельном изучении отдельных тем или вопросов по учебникам или учебным пособиям;
- в выполнении контрольных мероприятий по дисциплине;
- в подготовке рефератов

К самостоятельной работе по предмету относятся:

– самостоятельная работа на аудиторных занятиях (лекциях и практических занятиях);

– внеаудиторная самостоятельная работа.

Возможные виды самостоятельной работы студентов:

- проработка пройденных лекционных материалов по конспекту лекций, учебникам и пособиям на основании вопросов, подготовленных преподавателем;
- подготовка к проблемным лекциям;
- проработка дополнительных тем, не вошедших в лекционный материал, но обязательных согласно учебной программе дисциплины;
- подготовка к практическим занятиям;
- подготовка к промежуточному и итоговому контролю;
- подготовка научных докладов и творческих работ,
- выполнение индивидуальных работ;
- подготовка итогового отчета и презентации;

Методические рекомендации по выполнению отдельных видов работ

раскрывают:

- содержание и цели выполнения работы;
- исходную информацию;
- последовательность выполнения;
- требования к структуре и оформлению работы;
- порядок представления и защиты работы;
- критерии ее оценки.

Студентам задаются конкретные темы и вопросы для повторения и самостоятельного изучения. Целью ставится расширение и закрепление знаний и умений, приобретаемых студентом на традиционных формах занятий. Подготовка презентации и доклада по выбранной теме предполагает элементы творческого подхода.

В результате изучения дисциплины студенты должны получить базовые знания и навыки самостоятельной работы с информацией с использованием современного программного обеспечения

Основной формой учебной работы студентов являются практические занятия в компьютерном классе с использованием перечисленных выше программных средств. Для осознанного применения программных средств, студент должен в течение всего курса посещать лекций, в которых излагаются основные темы курса «Безопасность и защита информации», приводятся примеры решения задач на реальных данных.

В процессе выполнения практических и индивидуальных работ студент может использовать разработанные преподавателями кафедры учебные пособия, которые также можно применять и как справочник при самостоятельной работе с соответствующими программными средствами. Изучая материал по учебному пособию, студент должен переходить к следующему разделу только после усвоения предыдущего материала, проделывая все разобранные в пособии задания. В конце каждого занятия студенту предлагается ряд задач, для которых он должен дать правильную формальную постановку, получить с использованием программных средств результат и дать ему содержательную интерпретацию.

На лекциях и в процессе выполнения практических работ, полезно вести конспект, в котором рекомендуется выписывать определения, основные понятия, в логической последовательности их изложения, а также содержательные и формальные постановки решаемых задач и полученных результатов. На полях конспекта следует отмечать вопросы, по которым требуется консультация преподавателя. Записи в конспекте должны быть четкими, аккуратными и расположены в определенном порядке, соответствующем рабочей программе курса.

Если в процессе обучения у студентов возникают вопросы, разрешить которые самостоятельно не удается (неясность терминов, формулировок определений, в решении задач и пр.), то он может обратиться к преподавателю для получения у него устной или письменной консультации, а также консультации по компьютерной сети. Если студент не разобрался в теоретических вопросах по учебному пособию, то он может обратиться к

одному из учебников, указанных в списке литературы или к преподавателю.

6.6. Промежуточный контроль

Промежуточный контроль проводится в виде устного экзамена или итогового теста (по всему курсу, включая темы, изученные самостоятельно) в 5 семестре 3 курса. Максимальный балл за устный ответ на экзамене или итоговый тест составляет 50 баллов.

Допуск к экзамену – выполнение контрольных мероприятий 1-5. Рейтинговая оценка по дисциплине ставится на основании устного ответа, а также учета баллов текущего контроля.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Завгородний В.И. Комплексная защита информации в компьютерных системах. М.: Логос, 2001. - 264 с.

2. Зегжда П.П., Ивашко А.М.. Основы безопасности информационных систем. М.: Горячая линия-Телеком, 2000. - 452 с.

3. Информационная безопасность систем организационного управления: теоретические основы. В 2 т. Т. 1./ под ред. Н. А. Кузнецова, В. В. Кульбы ; Ин-т проблем передачи информации РАН. - М. : Наука, 2006. - 495 с.

4. Краковский, Ю. М. Информационная безопасность и защита информации: учеб. пособие:/ Ю.М. Краковский. - М. ; Ростов н/Д : МарТ, 2008. - 287 с.

5. Ярочкин, В.И. Информационная безопасность : учеб. для вузов: рек. М-вом образования РФ / В. И. Ярочкин. - 5- изд. - М. : Академический проект, 2008. - 543 с.

Нормативно-правовые документы (с учетом всех последующих изменений):

1. Конституция Российской Федерации 12 декабря 1993 г.
2. Справочно-правовая система «Консультант Плюс».
3. Справочно-правовая система «Гарант».

Дополнительная литература:

1. А.В. Аграновский, Р.А. Хади Практическая криптография: алгоритмы и их программи-рование – М.: СОЛОН-Пресс, 2002. - 256 с. – (Серия «Аспекты защиты»)

2. А.В. Домашев, В.О. Попов, Д.И. Правиков, И.В. Прокофьев, А.Ю. Щербаков Програм-мирование алгоритмов защиты информации. Учебное пособие. - М.: «Нолидж», 2000. - 288 с., ил.

3. Б.Ю. Анин Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 384 с., ил

4. Баричев С. Современные криптографические методы защиты информации.

5. Беляев А.В. Методы и средства защиты информации.

6. Компьютерра.Еженедельная газета.

7. Копылов В.А. Информационное право : учебник / В. А. Копылов. - Изд. 2-е, перераб. и доп. - М. : Юристъ, 2005. - 510 с.

8. Молдовян А.А. и др. Криптография. Спб.: Изд-во Лань, 2001. - 224 с.

9. Нечаев, В.И. Элементы криптографии : Основы теории защиты информации: Учеб.пособие / В. И. Нечаев. - М. : Высш. шк., 1999. - 109с.

Программное обеспечение и Интернет-ресурсы:

1. Безопасность в информационной сфере. [Электронный ресурс]. – Режим доступа: http://infosecurity.report.ru/

2. Библиотека информационной безопасности. [Электронный ресурс]. – Режим доступа: http://bib.pps.ru/

3. Библиотека сетевой безопасности [Электронный ресурс]. – Режим доступа: http://www.inattack.ru/

4. Защита и нападение в сети. [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru

5. Компьютерная безопасность и защита информации [Электронный ресурс]. – Режим доступа: https://securityvulns.ru/

6. Независимый российский информационно-аналитический центр, Интернет-проект, посвященный вопросам обеспечения информационной безопасности и противодействия вредоносному программному обеспечению. [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Мультимедийные средства и другая техника для презентаций учебного материала.

2. Компьютеры, принтер, сканер, интернет связь, программное обеспечение общего и профессионального назначения, комплект учебно-методической документации.