ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«СВЕТЛОГРАДСКИЙ ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ»

ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность
Специальность 230701 Прикладная информатика в образовании

2014 г.

Программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее - СПО) по специальности **230701 Прикладная информатика в образовании** базовой подготовки

Организация-разработчик: ГБОУ СПО Светлоградский педагогический колледж

Разработчики:

Сахарчук Н.О., преподаватель информатики ГБОУ СПО Светлоградский педагогический колледж

Рекомендовано методическим советом ГБОУ СПО «Светлоградский педагогический колледж» Ставропольский край

Заключение методического совета протокол № 1 от «29» августа 2014 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
Информационная безопасность

1.1. Область применения программы

Примерная программа учебной дисциплины является частью примерной основной профессиональной образовательной программы в соответствии с ФГОС по специальности (специальностям) СПО **230701 Прикладная информатика в образовании, базовой подготовки.**

Программа учебной дисциплины может быть использована в программах дополнительного профессионального образование и программах переподготовки, повышение квалификации по укрупненной группе специальностей СПО 230000 Информатика и вычислительная техника и предназначена для студентов, обучающихся по специальности 230701 Прикладная информатика (по отраслям).

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

П.00 Профессиональный цикл

ОП.00 Общепрофессиональные дисциплины, Вариативная часть

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

В результате освоения дисциплины обучающийся должен **уметь**:

- -Применять информационные системы безопасности в учебной и трудовой деятельности;
- Пользоваться различными системами безопасности информации в различных видах деятельности;
- Анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ.
- Использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной инфраструктуры.
- Применять эти методы для формирования и применения политик ИБ предприятия для эффективного управления процессами, работами и процедурами обеспечения ИБ.
- Ориентироваться в инфраструктуре проекта по разработке и внедрению средств, реализующих ИБ.

В результате освоения дисциплины обучающийся должен **знать**:

понятие информационных систем безопасности;

- роль мировых информационных систем безопасность в стратегии развития организации;
- признаки классификации безопасности информационных систем;
- основные типы функциональных систем безопасности ;

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося 120 часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося 78 часов;
самостоятельной работы обучающегося 42 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка	120
Обязательная аудиторная учебная нагрузка	78
в том числе:	
лабораторные занятия – не предусмотрено	-
практические занятия	39
контрольные работы	-
курсовая работа (проект) – не предусмотрено	-
Самостоятельная работа обучающегося (всего)	42
в том числе:	
установка, переустановка и создание образа ОС	18
поиск в интернете	4
операции над объектами ОС	10
сравнение процессов в ОС	4
настройка интерфейса ОС	6
Итоговая аттестация в форме дифференцированного зачета	

2.2. Тематический план дисциплины Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся		Объем часов	Уровень освоения
1	2		3	4
Раздел 1. Введение в информационную безопасность			**12**	
Тема 1.1 Основные понятия и определения информационной безопасности	**Содержание:**		6	
	1.	**История развития средств защиты информации.**		1
		Цели изучения, основные задачи, предмет и содержание курса «Информационная безопасность».		
		История развития средств защиты информации.		
	2.	**Определение информационной безопасности, угроз, уязвимости. Цели защиты.**		1
		Основные понятия и определения.		
		Определение информационной безопасности, угроз, уязвимости. Цели защиты.		
		Характеристики информации, применительно к задачам защиты.		
		Физические и экономические характеристики. Взаимосвязь между стоимостями.		
	3.	**Информационная безопасность в условиях функционирования в России глобальных сетей.**		1
		Информационная безопасность в условиях функционирования в России глобальных сетей.		
		Тенденции развития преступлений в сфере информационных технологий. Internet как среда для компьютерных преступлений.		
		Международные стандарты информационного обмена.		
Тема 1.2 Задачи и методы информационной безопасности.	**Содержание:**		4	
	1.	**Основные задачи информационной безопасности.**		1
	2.	**Основные методы обеспечения защиты информационной системы.**		1
		Законодательные, административные, технические.		1
		Классификация методов.		1

	Контрольная работа:		2	
	1.	Понятие несанкционированного доступа к информации		
	2.	Нормативно-правовые акты в области информационной безопасности РФ		
	3.	Методы обеспечения защиты ИБ		
Раздел 2. Угрозы информационной безопасности			**16**	
Тема 2.1 Понятие, определения и классификация угроз	**Содержание:**		4	
	1.	Ключевые свойства информации. Понятие угрозы. Целостность, конфиденциальность, доступность.		1
	2.	Определение и классификация угроз.		2
	3.	Угроза нарушения конфиденциальности. Служебная и предметная информация. Непрерывность защиты.		2
	4.	Угроза нарушения целостности. Статическая и динамическая целостность. Примеры нарушений целостности.		2
	5.	Угроза отказа служб. Классификация угроз и методы минимизации последствий.		2
Тема 2.2 Потенциальные противники и атаки	**Содержание:**		4	
	1.	**Виды противников или «нарушителей».**		1
		Классификация нарушителей: пользователи, хакеры, специальные агентства. Определение и характеристики хакеров.		2
		Виды и каналы утечки информации. Непосредственные и косвенные каналы. Каналы, предполагающие изменение структуры информационной структуры.		2
	2	**Классификация атак.**		1
		Классификации по месту возникновения, способу воздействия на информационную структуру, по направленности на компонент информационной системы.		2
		Характеристика атак систем управления базами данных и операционных систем.		2
		Сетевые атаки. Пассивная, отказ в обслуживании, модификация потока данных, создание ложного потока данных, повторное использование.		2
Тема 2.3	**Содержание:**		6	

Программно-технические методы защиты.	1.	**Программно-аппаратные средства защиты.**		2
		Основные аппаратные средства защиты. Основные программные средства защиты. Преимущества и недостатки программных средств защиты.		2
	2.	**Понятие информационного сервиса безопасности. Идентификация и аутентификация.**		
		Виды сервисов безопасности. Основные виды сервисов. Классификация видов сервисов.		
		Основные методы идентификации и аутентификации. Преимущества и недостатки парольной идентификации. Дополнительные меры защиты.		
		Биометрические показатели пользователей и возможности их применения. Основные методики идентификации по биометрическим показателям. Недостатки идентификации по биометрическим показателям.		
	3.	**Основы защиты корпоративных экономических информационных систем и Internet-подключений.**		
		Основные аспекты информационной безопасности корпоративных экономических информационных систем.		
		Потенциальные угрозы корпоративным ЭИС.		
		Основные положения обмена информацией в открытых сетях. Понятие межсетевого экрана.		
		Программные средства защиты Internet-подключений.		
	Самостоятельная работа:			
	1.	Сервисы управления доступом. Матрица списков доступа. Анализ дискреционного и мандатного доступа.		
	2.	Протоколирование и аудит. Задачи аудита. События, рекомендуемые для протоколирования.		
	3.	Журнал аудита. Активный аудит. Модели активного аудита. Двухуровневая модель аудита.		
Тема 2.4 Защита данных и сервисов от воздействия		**Содержание:**		
	1.	Вирусы. Виды вирусов. Определение вируса и программной закладки. Классификации вирусов.	0	

вредоносных программ		Антивирусное программное обеспечение. Методики обнаружения вирусов и виды антивирусного программного обеспечения. Недостатки антивирусов. Защита системы электронной почты. Спам. Определение спама, статистика угроз. Угрозы, связанные со спамом. Методики работы спамфильтров.		
	Практическое занятие:		2	
		Основные признаки присутствия на компьютере вредоносных программ		
Раздел 3. Теоретические основы защиты информации			**10**	
Тема 3.1. Основные положения теории информационной безопасности информационных систем.		**Содержание:**	6	
	1.	**Подходы к обеспечению информационной безопасности.**		
		Формулировка основных положений информационной безопасности.		
	2.	**Принципы обеспечения информационной безопасности.**		
		Системность, комплексность, непрерывность, разумная достаточность, гибкость, открытость алгоритмов, простота применения.		
	3.	**Формальные модели доступа к данным. Классификация моделей.**		
		Модель дискреционного доступа (DAC). Модель безопасности Белла-ЛаПадулы. Мандатная модель. Ролевая модель контроля доступа (RBAC). Системы разграничения доступа.		
		Монитор безопасности и его функции. Определение монитора безопасности. Характеристика основных функций.		
		Практическое занятие:	4	
		Создание и управление учетными записями пользователей		
Тема 3.2. Политика безопасности информационных систем.		**Содержание:**	4	
	1.	**Разделение политики безопасности по уровням.**		
		Административный уровень защиты информации. Описание функций административного уровня безопасности. Разработка и реализация политики безопасности. Итерационная процедура выработки политики безопасности. Функции политики безопасности по уровням. Вопросы, решаемые при разработке политики безопасности.		
	2.	**Анализ способов нарушений безопасности.**		

		Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ надежности и защищенности операционных систем разных семейств. Выявление недостатков этих операционных систем, приводящих к снижению уровня безопасности. Анализ и процентное соотношение успешности различных типов атак в разных операционных системах. Основные выводы о защищенности современных операционных систем.		
Раздел 4. Правовое обеспечение информационной безопасности			**6**	
Тема 4.1. Организационно-правовые методы информационной безопасности.		**Содержание:**	4	
	1.	**Организационно-правовые методы информационной безопасности**		
		Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Уровни правового обеспечения информационной безопасности. Перечисление документов и статей в них, касающихся вопросов информационной безопасности.		
		Место информационной безопасности экономических систем в национальной безопасности страны.		
		Национальная безопасность России, информационная безопасность в рамках национальной безопасности. Основные принципы обеспечения безопасности. Концепция информационной безопасности.		
		Доктрина информационной безопасности России. Четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.		
		Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Анализ недостатков информационной безопасности Российской Федерации.		
		Основные задачи обеспечения информационной безопасности. Правовые методы обеспечения информационной безопасности.		
	2.	**Общие сведения о документах предприятия, ориентированных на обеспечение информационной безопасности.**		
		Коммерческая тайна. Требования по защите коммерческой тайны в		

		документах предприятия. Конфиденциальная тайна Требования по защите конфиденциальной информации в документах предприятия.		
Тема 4.2. Стандарты обеспечения информационной безопасности.		**Содержание:**	2	
	1.	Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”).		
		Понятие оценочного стандарта. Основные положения "Оранжевой книги".		
		Критерии степени доверия и требования безопасности.		
		Руководящие документы Гостехкомиссии России.		
		Классы защищенности, группы и классы пользователей, их права и возможности.		
		Международные стандарты информационной безопасности.		
		Стандарт ISO/IEC 15408 "Общие критерии". Описание требований безопасности и характеристик угроз.		
		Классы функциональных требований. Классификационная статистика.		
		Использование защищенных компьютерных систем.		
		Практические занятия:	4	
		Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS		
Раздел 5 Криптографические методы защиты информации				
Тема 5.1. Основные понятия криптографии.		**Содержание:**		
	1.	Понятие криптографии, шифра, ключа, взлома шифра.	4	
	2.	Задачи и методы криптографии. Секретность, аутентификация, целостность, неоспоримость.		
	3.	Виды шифров. Симметричные, ассиметричные, блочные и потоковые шифры. Принцип Керкхоффса.		
	4.	Алгоритм шифрования DES. Основные режимы работы алгоритма DES (электронная кодовая книга, сцепление блоков шифра). Области применения алгоритма DES.		
	5.	Комбинирование блочных алгоритмов. Блочные и поточные шифры.		
	6.	Асимметричные криптосистемы. Модулярная арифметика.		
	7.	Концепция криптосистемы с открытым ключом. Однонаправленные функции.		

	8.	Криптосистема шифрования RSA. Комбинированный метод шифрования.		
	9.	Криптографические примитивы. Хэш-функция и её применения.		
	10.	Генераторы псевдослучайных чисел.		
Тема 5.2. Криптографические протоколы.		**Содержание:**	4	
	1.	**Основные криптографические протоколы. Вспомогательные криптографические протоколы.**	2	
		Понятие протокола. Определение протокола, условия протоколов. Виды протоколов.		
		Схема обмена ключами, аутентификация, распределение ответственности, цифровая подпись.		
		Электронная цифровая подпись. Задачи, решаемые цифровой подписью. Схема создания и проверки электронной цифровой подписи.		
	2.	**Модели основных криптоаналитических атак.**	2	
		Атака методом сведения к середине. Словарная атака Четыре основных подхода к анализу криптографических протоколов		
		Практические занятия:		
	1.	Повышение безопасности информации встроенными средствами шифрования операционной системы	4	
	2.	Программирование арифметических алгоритмов	2	
	3.	Программирование алгебраических алгоритмов	2	
	4.	Защита от закладок при разработке программ	2	
Тема 5.3. Основные технологии построения защищённых экономических информационных систем.		**Содержание:**	4	
	1.	**Общие принципы построения защищенных систем.**	2	
		Выдержки из открытой концепции "Защищенные информационные системы. Информационный документ корпорации Microsoft." Цели защищенных информационных систем: безопасность, безотказность, деловая добросовестность.		
	2.	**Средства разработки и правила их реализации.**	2	
		Основные средства, методика их реализации, практические аспекты функционирования. Фундаментальные проблемы, возникающие при построении		

		защищенных информационных систем. Политические вопросы, технические и социальные аспекты.		
Тема 5.4. Повышение безопасности информации встроенными средствами шифрования операционной системы		**Содержание:**	2	
		Общие сведения о настройке параметров безопасности		
		Настройка политик учетных записей		
		Завершение работы компьютера без регистрации в системе		
	Самостоятельная работа:		8	
		Виды угроз безопасности ЭИС	4	
		Методы и средства защиты ЭИС	2	
		Развитие электронных платежных систем	2	
Раздел 6 Защита информации в электронных платежных системах				
Тема 6.1. Элементы платежной системы и их защита		**Содержание:**	2	
	1.	Принципы функционирования электронных платежных систем.		
	2.	Электронные пластиковые карты.		
	3.	Обеспечение безопасности систем POS.		
	4.	Обеспечение безопасности банкоматов.		
Тема 6.2. Универсальная электронная платежная система UEPS		**Содержание:**	2	
	1.	Состав и архитектура платежной системы.		
	2.	Распределение ключей и паролей.		
	3.	Цикл платежной транзакции.		
	4.	Торговые терминалы.		
	5.	Формирование сессионных ключей.		
	6.	Эмиссия карточек.		
	7.	Разграничение ответственности между банками-участниками платежной системы		
		Практические занятия:	6	
	1.	Настройка системных параметров безопасности	2	
	2.	Архивация и восстановление данных	2	
	3.	Аудит ресурсов и событий системы защиты	2	
Тема 6.3. Безопасность электронных платежей через Internet		**Содержание:**	2	
	1.	Состав и архитектура платежной системы.		
	2.	Распределение ключей и паролей.		

	3.	Цикл платежной транзакции.		
	4.	Торговые терминалы. Формирование сессионных ключей. Эмиссия карточек.		
	5.	Разграничение ответственности между банками-участниками платежной системы.		
Тема 6.4. Настройка системных параметров безопасности. Архивация и восстановление данных.		**Содержание:**	2	
	1.	Настройка системных параметров безопасности		
	2.	Архивация и восстановление данных		
Тема 6.5. Аудит ресурсов и событий системы защиты		**Содержание:**	2	
	1.	Аудит ресурсов и событий системы защиты		
		Практические занятия:	8	
	1.	Универсальная электронная платежная система UEPS	2	
	2.	Безопасность электронных платежей через Internet	2	
	3.	Настройка системных параметров безопасности. Архивация и восстановление данных.	2	
	4.	Аудит ресурсов и событий системы защиты	2	
Раздел 7. Защита информации в образовательных системах				
Тема 7.1. Обзор российского законодательства в области защиты персональных данных.		**Содержание:**	2	
	1.	Понятие "персональные данные"		
	2.	Алгоритм организации системы защиты персональных данных		
	3.	Федеральный закон «О персональных данных»		
Тема 7.2. Угрозы безопасности персональных данных		**Содержание:**	2	
	1.	Базовая модель содержания угроз безопасности персональных данных при их обработке в ИСПДн		
	2.	Классификация угроз безопасности персональных данных		
	3.	Характеристика угроз НСД в ИСПДн		
	4.	Характеристика уязвимостей ИСПДн		
Тема 7.3. Методы и способы защиты информации в информационных		**Содержание:**	2	
	1.	Классификация методов и способов ЗИ в ИСПДн		
	2.	Методы и способы защиты информации от несанкционированного доступа		

системах защиты персональных данных.	3.	Методы и способы защиты информации от утечки по техническим каналам		
	4.	Безопасное межсетевое взаимодействие для информационных систем		
	5.	Анализ защищенности		
Тема 7.4. Информационная безопасность образовательного учреждения.		**Практические занятия:**	4	
	1.	Особенности обеспечения информационной безопасности в образовательных учреждениях	2	
	2.	Современное состояние обеспечения информационной безопасности в образовательных учреждениях	2	
		Всего:	120	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета операционных систем и сред. Стандартное оборудование лекционного и компьютерного класса с проектором и экраном.

Оборудование учебного кабинета иностранного языка:

- Магнитно-маркерная доска (3 секции)
- Стенка для учебно-методических материалов (3 секции)
- Рабочее место преподавателя;
- Рабочие места обучающихся не менее 15;
- Учебная, методическая, справочная литература, словари, раздаточный материал, материалы для контроля (тесты, тексты с заданиями и др.)
- Комплект учебно-наглядных пособий
- Лицензионное базовое программное обеспечение;
- Лицензионное специальное программное обеспечение;

Технические средства обучения:

- проектор;
- интерактивная доска (проекционный экран);
- персональные компьютеры с выходом в интернет;
- акустическая система;
- LAN;
- диски DVD-RW.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники (ОИ):

№ п/п	*Наименование*	*Автор*	*Издательство, год издания*
ОИ 1	*Информационные технологии: открытые системы, сети, безопасность в системах и сетях*	*Барабанова М.И., Кияев В.И.*	*СПб, изд-во СПбГУЭФ, 2010*
ОИ 2	*Информационная безопасность.*	*Партыка Т.П., Попов И.И.*	*М:, ФОРУМ, 2010*
ОИ 3	*Теоретические основы защиты информации:*	*Корт С.С.*	*М.: Гелиос АРВ, 2004.-240с*
ОИ 4	*Защита информации в распределенных корпоративных сетях и системах.*	*Соколов А.В., Шаньгин В.Ф.*	*М.:ДМК Пресс-Ю 2002.-656 с*
ОИ 5	*Основы информационной безопасности автоматизированных систем*	*В.Л. Цирлов*	*Феникс, 2008*

Дополнительные источники (ДИ):

№ п/п	*Наименование*	*Автор*	*Издательство, год издания*
ДИ 1	*Основы информационной безопасности.*	*Галатенко В.А.*	*М:, ИНТУИТ, 2006, 208 с.*
ДИ 2	*Безопасность в сетях Internet и Intranet.*	*Левин М.*	*М:, Познавательная книга плюс, 2001, 320 с.*
ДИ 3	Практическая криптография	*Нильс Фергюсон, Брюс Шнайер*	*М.: Издательский дом «Вильямс», 2005г.-424с.*
ДИ 4	*Энциклопедия компьютерных вирусов.*	*Козлов Д.А., Парандовский А.А., Парандовский А.К.*	*М.:СОЛОН-Р, 2001. - 461 с.*
ДИ 5	*Безопасность программного обеспечения компьютерных систем. –*	*Казарин О. В.*	*М.: МГУЛ, 2003. – 212 с.*
ДИ 6	*Методы и средства защиты информации.*	*Хорошко В. А., Чекатков А. А.*	*М.: Юниор, 2003. – 504 с.*
ДИ 7	*Информационная безопасность и защита информации. Конспект лекций.*	*Будко В. Н.*	*Воронеж: ВГУ, 2003. – 86 с.*
ДИ 8	*Основы защиты информации*	*Куприянов А.И., А.В. Сахаров*	*М.: Академия, 2006, 256с.*

Интернет-ресурсы (И-Р)

И-Р 1.www. infosec.ru
И-Р 2. www.securitylab.ru
И-Р 3. www.cnews.ru
И-Р 4. www.citforum.ru
И-Р 5. www.osp.ru
И-Р 6. www.ccc.ru
И-Р 7. www.fstek.ru
И-Р 8. http://www.avp.ru
И-Р 9. http://www.viruslist.com/virusHst.asp

Основные источники:

1. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях (Учебное пособие). – СПб, изд-во СПбГУЭФ, 2010, 270 с.
2. Партыка Т.П., Попов И.И. Информационная безопасность. – М:, ФОРУМ, 2010, 432 с.

Дополнительная литература

1. Галатенко В.А. Основы информационной безопасности. – М:, ИНТУИТ, 2006, 208 с.
2. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М:, Горячая линия – Телеком, 2000, 452 с.
3. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М,: ДМК Пресс, 2002, 656 с.
4. Астахов А.Н. Анализ защищенности корпоративных систем. – «Открытые системы», 2002, № 7,8.
5. Левин М. Безопасность в сетях Internet и Intranet. – М:, Познавательная книга плюс, 2001, 320 с.
6. Ховард М., Лебланк Д. Защищенный код. – М:, изд-во «Русская Редакция», 2005, 704 с.
7. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1997. – 336с.
8. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
9. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
10. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001 г.
11. Масленников А. Практическая криптография BHV – СПб 2003 г.
12. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002 г.
13. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002 г.

1. Козлов Д.А., Парандовский А.А., Парандовский А.К. Энциклопедия компьютерных вирусов. - М.:СОЛОН-Р, 2001. - 461 с.

В энциклопедии собрана исчерпывающая информация по проблеме компьютерных вирусов, от создания до обнаружения и уничтожения. Приведены примеры написания и уничтожения COM-,EXE-,Boot-, Internet- и макровирусов, как нерезидентных, так резидентных и полиморфных. Основное преимущество данной книги в ее практическом применении.

2.http://www.avp.ru - сервер антивирусной лаборатории Евгения Касперског 6.0, на котором имеется возможность бесплатно и быстро проверить файлы на наличие вирусного кода. В разделе «Триальные версии» вы можете познакомиться с

антивирусными продуктами Лаборатории Касперского перед приобретением.

3. **http://www.viruslist.com/virusHst.asp** - раздел сервера антивирусной лаборатории Евгения Касперского, содержащий огромное число описаний вирусов и демонстраций вызываемых вирусами эффектов, классификацию вирусов, общие методы обнаружения и удаления компьютерных вирусов.

4. **http://www.dials.ru** - сервер антивирусной лаборатории «Лаборатория Данилова» и «ДиалогНаука». На данном сервере вы можете:найти информацию о программах сканер Doctor Web; резидентный сторож SpIDer Guard; ревизор дисков ADinf и универсальный лекарь ADinf Cure Module, выполнить через Интернет бесплатно удаленную проверку ваших файлов на наличие вирусов с помощью последней версии антивирусного сканера Doctor Web, а также получить некоммерческие версии антивирусных продуктов, дополнения для программы Doctor Web и документацию.

5. **http://www.adinf.ru** - WEB-сайт разработчиков антивируса ADinf.

6. **http://www.symantec.ru** - Российское Интернет-представительство компании Symantec, производящей антивирусный пакет Norton Anti Virus.

3.3. Электронные издания, цифровые образовательные ресурсы

Интернет-ресурсы:

1. www. infosec.ru
2. www.securitylab.ru
3. www.cnews.ru
4. www.citforum.ru
5. www.osp.ru
6. www.ccc.ru
7. www.fstek.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Уметь:	
Анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ.	Оценка выполнения практического задания на экзамене
	Оценка результатов наблюдения за деятельностью студентов на практическом занятии
Использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной инфраструктуры.	Оценка результатов наблюдения за деятельностью студентов на практическом занятии
Применять эти методы для формирования и применения политик ИБ предприятия для эффективного управления процессами, работами и процедурами обеспечения ИБ.	Оценка выполнения практического задания на экзамене
Ориентироваться в инфраструктуре проекта по разработке и внедрению средств, реализующих ИБ.	Оценка результатов наблюдения за деятельностью студентов на практическом занятии
Знать:	
Предпосылки формирования сферы знаний по информационной безопасности; законодательную и нормативную базу ИБ;	Контрольные работы по разделам
основные меры, направленные на обеспечение ИБ на различных уровнях деятельности современного предприятия;	
иметь полное представление о значение информационной безопасности для современного бизнеса,	
о перспективах развития технологий обеспечения информационной безопасности.	

Практические занятия (семинары)

Практическая работа по данному курсу проводится в виде ролевой деловой игры «Разработка элементов информационной защиты современного высокотехнологичного предприятия».

Эта игра продолжает деловую игру по разработке модели современной компании и её бизнес-процесса по разработке программного обеспечения, которая проводилась этими студентами в 5-м семестре. В данном случае группы студентов, которые построили модель компании по разработке ПО, строят модель информационной безопасности для своих компаний. Модель ИБ включает в себя концепцию, программу и политику ИБ, модель угроз, модель защиты данных и информации. В результате должна быть разработана модель комплексной защиты информационной инфраструктуры компании.

Темы семинарских занятий включают:

Тема 1. Подготовка предварительного варианта концепции информационной безопасности компании

Тема 2. Построение структуры нормативно-правовых документов деятельности компании на базе российского законодательства в сфере информационного права.

Тема 3. Подготовка описания охраняемой информации, «портрета» нарушителя, модели угроз, построение модели информационной безопасности

Тема 4. Разработка параметров защищенности программных и информационных систем компании и программы ИБ

Тема 5. Разработка модели общей и частных политик информационной безопасности компании. Подготовка нормативного документа для введения в действия политики ИБ.

Тема 6. Описание структуры информационных рисков, построение модели процесса оценки рисков, составление списка мероприятий для уменьшения рисков. Обзор программных продуктов для оценки информационных рисков.

Тема 7. Формирование опорной системы стандартов для реализации информационной безопасности предприятия.

Тема 8. Подготовка базовой совокупности сервисов информационной защиты. Выбор и внедрение средств криптографической защиты информации.

Тема 9. Формирование программно-аппаратных и технических средств защиты информационных ресурсов от внешних атак и вирусной опасности. Построение комплексной системы информационной защиты.

Отчётным материалом является сайт компании, на котором представлены результаты деловой игры. На каждом практическом занятии (семинаре) заслушиваются доклады всех групп, сопровождаемые презентациями о пошаговой реализации модели ИБ.