МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный педагогический университет»
(ТГПУ)

УТВЕРЖДАЮ
Проректор по учебной работе (декан)
_____
«01» 09 2011 г.

ПРОГРАММА ДИСЦИПЛИНЫ

ДПП.03 ИНФОРМАЦИОННАЯ ЗАЩИТА

Томск-2011

1. Цели и задачи дисциплины:

Цель дисциплины – заложить терминологический фундамент, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, приобрести навыки анализа угроз информационной безопасности, рассмотреть основные общеметодологические принципы теории информационной безопасности.

Основные задачи дисциплины:

- ознакомление студентов с терминологией информационной безопасности;
- развитие мышления студентов;
- изучение методов и средств обеспечения информационной безопасности;
- обучение определению причин, видов, источников и каналов утечки, искажения информации.

2. Требования к уровню освоения содержания дисциплины:

В результате изучения дисциплины студенты должны:

а) знать:

- основные понятия Федерального закона;
- Государственную систему правового обеспечения защиты информации в Российской Федерации;
- информационные системы;
- основные направления государственной политики в сфере информатизации;
- причины нарушения целостности информации;
- виды потерь.

б) уметь:

- определять виды угроз информационным системам;
- классифицировать и характеризовать каналы утечки информации.

3. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестры	
		4	5
Общая трудоемкость дисциплины	260	140	120
Аудиторные занятия	185	95	90
Лекции	74	38	36
Практические занятия (семинары)	0	0	0
Лабораторные работы	111	57	54
Другие виды аудиторных занятий			
Самостоятельная работа	75	45	30
Курсовая работа (реферат)			
Вид итогового контроля		зачет	экзамен

4. Содержание дисциплины

4.1.Разделы дисциплины и виды занятий

№ п/п	Раздел дисциплины	Лекции	Практические занятия	Лабораторные работы
4 семестр				
1	Информационная безопасность в структуре РФ.	6		10
2	Информация как стратегический национальный ресурс, информационная инфраструктура, основные факторы, влияющие на состояние информационной безопасности в РФ.	6		14
3	Основные направления и положения; национальные интересы РФ в информационной сфере, их правовое, материальное и организационно-техническое обеспечение.	4		6
4	Правовые основы информационной безопасности личности, общества, государства, основные нормативно-правовые документы.	6		18
5	Правовые аспекты информационной безопасности.	4		2
6	Виды и источники угроз ИБ РФ, методы обеспечения ИБ РФ.	12		7
	Итого	38		57
5 семестр				
7	Классификация и краткая характеристика каналов утечки информации.	10		4
8	Методы и средства защиты информации.	12		40
9	Информационные войны, формы и методы информационной агрессии.	8		
10	Социально-политические манипуляции личностью и механизмы защиты.	6		10
	Итого	36		54
	Всего	74		111

4.2. Содержание разделов дисциплины.

Раздел 1. Информационная безопасность в структуре РФ.

Лекции 1-3

Понятие информации. Виды и свойства информации. Структура информационного процесса. Окружающая среда как источник информации. Восприятие информации человеком. Особенности восприятия окружающей среды человеком. Перенасыщенная информацией среда. Роль информации в развитии общества. Информационные революции. Информационное общество. Проблема информационного неравенства. Россия в информационной эпохе.

Образование в информационном обществе. Особенности обучения в информационном обществе. Компетентность педагога в информационном обществе. Информационная пассивность педагога.

Раздел 2. Информация как стратегический национальный ресурс, информационная инфраструктура, основные факторы, влияющие на состояние информационной безопасности в РФ.

Лекции 4-6

Определение понятия «информационная безопасность». История ИБ. Информационное противостояние от древности до Нового времени. Составляющие информационной безопасности. Составляющие национальных интересов РФ в информационной сфере. Национальные интересы РФ в информационной сфере. Виды угроз информационной безопасности РФ. Источники угроз информационной безопасности РФ. Основные цели и задачи обеспечения информационной безопасности РФ. Объекты информационной безопасности РФ.

Раздел 3. Основные направления и положения; национальные интересы РФ в информационной сфере, их правовое, материальное и организационно-техническое обеспечение.

Лекции 7, 8

Основные положения государственной политики обеспечения ИБ РФ. Система обеспечения ИБ РФ, ее основные функции и организационные основы. Общие методы обеспечения ИБ РФ. Источники угроз ИБ РФ. Защита информации в экономике, внутренней и внешней политике, науке и технике. Информационное обеспечение оборонных мероприятий и боевых действий. Безопасность в сфере духовной жизни человека и общества. Важность и сложность проблемы ИБ.

Раздел 4. Правовые основы информационной безопасности личности, общества, государства, основные нормативно-правовые документы.

Лекции 9-11

Правовое регулирование открытых информационных ресурсов. Защита информации институтом интеллектуальной собственности. Охрана результатов творческой деятельности. Объекты интеллектуальной собственности. Промышленная собственность. Российский и зарубежный опыт охраны интеллектуальной собственности. Международные правовые акты. Торговый знак, знак обслуживания, торговая марка, фирменное наименование, эмблема предприятия. Страхование ценной информации. Законодательные акты, охраняющие вещную собственность на документированную информацию.

Раздел 5. Правовые аспекты информационной безопасности.

Лекции 12, 13

Правовая защита информационных ресурсов ограниченного доступа. Понятие тайны, секрета, конфиденциальности. Направления и методы защиты тайны в дореволюционной России и зарубежных странах. Институт тайн в законодательстве Российской Федерации. Защита информации институтом государственной тайны. Субъекты и объекты информационных правоотношений в области государственной тайны. Отнесение сведений к государственной тайне и их засекречивание. Распоряжение сведениями, составляющими государственную тайну. Рассекречивание сведений и их носителей. Понятия - "фирменные секреты", "технологические секреты (ноу-хау)", "научные секреты (ноу-ноу)". Понятие конфиденциальности как определение сферы несекретной информации ограниченного доступа. Сущность термина, особенности и условия применения, дискуссионность.

Правовые и технологические аспекты присвоения информации категории конфиденциальной. Конфиденциальная информация и ее виды. Персональные данные. Ограничения на отнесение информации к категории конфиденциальной.

Международное сотрудничество России в области обеспечения информационной безопасности. Виды коммерческих международных операций. Возможные условия разглашения сведений, составляющих коммерческую тайну. Организация работы с зарубежными партнерами. Конфиденциальность при работе с зарубежными партнерами. Научно-техническое сотрудничество.

Раздел 6. Виды и источники угроз ИБ РФ, методы обеспечения ИБ РФ.

Лекции 14-19

Основные направления и этапы работ по созданию комплексной системы безопасности предприятия (фирмы). Понятие аналитической работы, ее цели и задачи. Аналитическая работа по выявлению каналов несанкционированного доступа к информации. Аналитическая работа с источником конфиденциальной информации. Аналитическая работа с источником угрозы конфиденциальной информации. Аналитическая работа с каналом объективного распространения информации. Стадии аналитической работы. Порядок и методика сбора исходных сведений, их анализа и оценки. Экспертные системы. Результаты аналитической работы как основа формирования системы защиты информации и ее совершенствования. Содержание элемента криптографической защиты информации. Формирование и актуализация системы в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом предпринимательской структуры и видами угроз. Система защиты информации в малом бизнесе. Стоимость системы и критерии выбора системы. Сертификация систем и средств защиты информационных систем и информационных ресурсов.

Регламентация технологии работы персонала фирмы с документами, вычислительной и организационной техникой, средствами связи. Регламентация работы с персоналом. Регламентация системы охраны фирмы. Регламентация защиты информации в экстремальных ситуациях. Состав методических указаний, правил, памяток, схем и иных наглядных пособий.

Основные направления деятельности службы безопасности предприятия (фирмы) по защите информационных ресурсов. Виды служб безопасности, их место в аппарате управления предпринимательских структур различных типов. Менеджер по безопасности. Задачи службы безопасности, основные функции. Руководство и подчиненность. Типовая структура службы безопасности. Место, задачи, функции и структура подразделения (или службы) конфиденциальной документации. Регламентированный и нерегламентированный контроль системы защиты. Цели и задачи планирования работы по формированию и совершенствованию системы защиты информации. Планирование работы службы. Стадии контроля; учет контрольных операций.

Угрозы безопасности информации от персонала и направления ее защиты. Психологические особенности личности человека, владеющего тайной. Задачи и стадии работы с персоналом, обладающим конфиденциальными сведениями. Особенности приема (перевода) сотрудников на работу, связанную с владением конфиденциальной информацией. Принципы подбора персонала. Технологическая цепочка - этапы, процедуры и методы подбора. Состав документов, получаемых от кандидата на должность, анализ документов. Особенности проведения собеседования, анкетирования, тестирования и опроса. Критерии отбора кандидатов на должность. Особенности документирования приема или перевода на должность. Формы обязательств о неразглашении тайны фирмы. Особенности содержательной части контракта. Особенности оформления приема на работу сотрудников, непосредственно не связанных с тайной фирмы.

Доступ персонала к конфиденциальным сведениям, документам и базам данных. Цели

и задачи разрешительной (разграничительной) системы доступа персонала и иных лиц к конфиденциальным сведениям, документам, базам данных и продукции. Структура разрешительной системы и ее связь с требованиями деловой целесообразности и персональной ответственности руководителей и сотрудников за сохранность тайны фирмы. Регистрация (протоколирование) фактов доступа. Несанкционированный доступ. Порядок доступа к конфиденциальным сведениям представителей других фирм и служащих государственных учреждений. Контроль за доступом.

5 семестр

Раздел 7. Классификация и краткая характеристика каналов утечки информации.

Лекции 20-24

Устройства и системы противоправного преднамеренного овладения конфиденциальной информацией. Технические средства защиты объектов. Инженерно-техническая защита. Системы охранной сигнализации на территории и в помещениях объекта обработки информации. Требования к системам охранной сигнализации. Наружные системы охраны и охранной (пожарной) сигнализации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Биометрия, интеллектуальные карты.

Раздел 8. Методы и средства защиты информации.

Лекции 25-30

Классы задач защиты информации. Способы и средства защиты информации. Криптографические методы защиты информации.

Компьютерные преступления. Особенности компьютерных преступлений. Уголовно-правовая характеристика компьютерных преступлений. Криминалистическая характеристика компьютерных преступлений. Предотвращение и раскрытие компьютерных преступлений.

Компьютерные вирусы. Определение компьютерного вируса. Основные признаки вирусного поражения. Понятия о видах вирусов. Классификация по среде обитания вируса; по способу заражения среды обитания; по деструктивным возможностям; по особенностям алгоритма вируса. Методы борьбы с вирусами. Обзор антивирусных программ.

Основы безопасности в Internet. Угрозы. Классификация удаленных атак: по сценарию, по цели, по характеру взаимодействия с жертвой. Удаленный сбор информации. Выяснение адресов. Поиск уязвимостей. Наиболее распространенные классы удаленных атак. Вирусы и троянские программы. Отказ в обслуживании. Переполнение буфера. Пассивные атаки. Обзор программных средств защиты. Сканеры уязвимости. Системы и технологии обнаружения атак. Программные шлюзы и прокси-серверы. Internet-серверы. Межсетевые экраны. Функции межсетевого экранирования. Фильтрация трафика. Средства защиты трафика.

Электронная почта и ее защита. Безопасность электронной почты. Методы обеспечения конфиденциальности переписки. Защита шифрованием, средства шифрования. Линейное шифрование. Абонентское шифрование. Индивидуальная и корпоративная защита от спама и почтовых вирусов. Электронные платежи, использование кредитных карт. Виды мошенничества. Средства идентификации и аутентификации.

Раздел 9. Информационные войны, формы и методы информационной агрессии.

Лекции 31-34

Сущность и современное состояние манипуляции сознанием и поведением людей. Основные методы и средства информационного воздействия на человека. Мифы как инструмент воздействия на людей. Манипулятивные технологии в избирательных кампаниях Методы тоталитарных сект и способы защиты от них.

Информационная безопасность в повседневной жизни. Рыночные отношения – социально-экономическая основа манипуляции людьми. Влияние средств массовой информации на мировоззрение людей и духовно-нравственное становление подрастающих поколений. Повседневно-бытовой уровень манипуляции сознанием. Защита русского языка – важное условие информационной безопасности России. Средства информационного воздействия и защита здоровья.

Глобальное общество и проблемы информационной безопасности. Объективные и субъективные предпосылки создания глобального общества. Интернета в мировом информационном пространстве. Глобальные ожидания и опасения человечества.

Слухи как неформальный обмен информацией. Слухи как социально-психологический феномен. Определение слуха. Классификация слухов. Причины возникновения и механизмы распространения слухов. Управление слухами. Особенности распространения слухов в чрезвычайных ситуациях.

Информационные и психологические войны. Понятие информационной войны. Информационное оружие. Информационная атака. Стратегическое информационное противоборство. Понятие психологической войны. Цели психологической войны. Психологическая война в истории человечества. Использование пропаганды во второй мировой войне. Психологическая операция. Виды психологического воздействия. Средства психологического воздействия. Инструментарий психологических операций.

Раздел 10. Социально-политические манипуляции личностью и механизмы защиты.

Лекции 35-37

Неприкосновенность частной жизни граждан. Угрозы неприкосновенности частной жизни граждан. Кодекс справедливого использования информации.

Влияние средств массовой информации на человека. Методы влияния СМИ на человеческое сознание. Влияние телевидения на детей. Влияние просмотра сцен насилия по телевидению на поведение человека. Влияние рекламы на человека. Понятие рекламы. Влияние рекламы на детей. Особенности рекламы для детей в различных странах. Приемы рекламного воздействия. Реклама нездорового образа жизни.

Интернет и безопасность детей. Опасности сети Интернет. Интернет-зависимость в подростковой среде. Жестокие компьютерные игры. Опасность жестоких компьютерных игр. Влияние жестоких компьютерных игр на поведение человека.

5. Лабораторный практикум.

№ п/п	Раздел	Наименование лабораторной работы	Количество часов
4 семестр			
1.	1	Конфиденциальная информация.	2
2.	1	Россия в информационной эпохе.	2
3.	1	Информационная пассивность педагога.	2
4.	1	Права на доступ к информации.	4
5.	2	Государственная тайна и системы ее защиты.	2
6.	2	Изучение концепции защиты информации.	4
7.	2	Изучение эволюции понятий «государственная тайна» и	4

		«военная тайна» в период экономических реформ 1985 – 2009 годов.	
8.	2	Изучение Доктрины информационной безопасности РФ.	4
9.	3	Информационные войны XX века.	2
10.	3	Обеспечение информационной безопасности в правоохранительной сфере и при возникновении чрезвычайных ситуаций.	4
11.	4	Изучение Конституции РФ. Федеральное законодательство в сфере информационной безопасности. Указы Президента РФ и иные нормативно-правовые акты по вопросам информационной безопасности.	6
12.	4	Ответственность за нарушение законодательства о средствах массовой информации.	2
13.	4	Служебная тайна. Производственная тайна.	2
14.	4	Предпринимательская (коммерческая) тайна как форма защиты ценной деловой и производственной предпринимательской информации.	4
15.	4	Профессиональная тайна. Банковская тайна. Тайны личная и семейная.	4
16.	5	Изучение международных и государственных стандартов информационной безопасности.	2
17.	6	Изучение основных направлений деятельности службы безопасности предприятия (фирмы) по защите информационных ресурсов.	4
18.	6	Анализ особенностей работы с персоналом, владеющим конфиденциальной информацией.	3
		Итого	57
5 семестр			
1.	7	Защита от закладок при разработке программ	4
2.	8	Шифр Цезаря.	4
3.	8	Шифр Плейфейера.	4
4.	8	Архивирование текста.	4
5.	8	Методы шифрации текста в рисунок.	4
6.	8	Шифр «Лесенка».	4
7.	8	Метод вертикальной перестановки.	4
8.	8	Шифр Виженера.	4
9.	8	Метод поворотной решётки.	4
10.	8	Комбинация методов	4
11.	8	Профилактика заражения вирусами компьютерных систем	4
12.	10	Роль рекламы в манипуляции сознанием людей.	4
13.	10	Изучение Кодекса справедливого использования информации.	2
14.	10	Интернет-зависимость в подростковой среде.	4
		Итого	54

6. Учебно - методическое обеспечение дисциплины

6.1. Рекомендуемая литература

а) основная

1. Мельников, В. П. Информационная безопасность и защита информации : учебное пособие для вузов / В. П. Мельников и др. ; под ред. С. А. Клейменова. – М. : Академия, 2011. – 330 с.
2. Казанцев, С. Я. Правовое обеспечение информационной безопасности : учебное пособие для вузов / С. Я. Казанцев и др. ; под ред. С. Я. Казанцева. – М. : Академия. 2008. – 238 с.
3. Шереметьева У. М. Информационная безопасность: Конспект лекций / У.М. Шереметьева. – Томск : Издательство Томского государственного педагогического университета, 2009. – 133 с.

б) дополнительная

1. Арутюнов, В. В. Защита информации : учебно-методическое пособие / В. В. Арутюнов. - М. : Либерея-Бибинформ, 2008. – 55 с.
2. Куприянов, А. И. Основы защиты информации : учебное пособие для вузов / А. И. Куприянов и др. – М. : Академия, 2006. – 256 с.
3. Молдовян, Н. А. Теоретический минимум и алгоритмы цифровой подписи : учебное пособие / Н. А. Молдовян. – СПб. : БХВ-Петербург, 2010. – 289 с.
4. Информационное общество : Информационные войны. Информационное управление. Информационная безопасность / С. М. Виноградова и др. ; под ред. М. А. Вуса. – СПб. : Издательство СПбГУ, 1999. – 212 с.
5. Одинцов, А. А. Экономическая и информационная безопасность предпринимательства : учебное пособие для вузов/А. А. Одинцов. – М. : Академия, 2008. – 333 с.
6. Ярочкин, В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. – М. : Академический Проект, 2003. – 638 с.

6.2. Средства обеспечения дисциплины

Учебники и учебно-методические пособия, тесты.

7. Материально-техническое обеспечение дисциплины

Учебный класс, компьютерный класс с выходом в Интернет, компьютерная программа тестирования.

Следующие электронные ресурсы:

1. Иллюстрированный самоучитель по защите информации [Электронный ресурс] – Режим доступа : proklondike.com.

Иллюстрированный самоучитель по разработке безопасности [Электронный ресурс] – Режим доступа : proklondike.com.

2. Леонтьев, Б. К. Как ломают телефонные сети [Электронный ресурс] : пособие по взлому и защите телефонных сетей / Б. Леонтьев, 2006. – 320 с. – Режим доступа : http: //proklondike.com.

3. Информационная безопасность [Электронный ресурс]. – Режим доступа : http: // iqlib.ru.

8. Методические рекомендации и указания по организации изучения дисциплины.

8.1. Методические рекомендации преподавателю

Примерным учебным планом на изучение дисциплины отводится два семестра. Учебная работа проводится в форме лекций, лабораторных работ и самостоятельной работы.

Система контроля знаний и умений включает устные и письменные формы. В том числе: реферативные сообщения, выполнение тестовых заданий, контрольных работ.

Лекции проводятся в традиционной форме.

Задания для самостоятельной работы раздаются студентам в начале изучения дисциплины и сдаются в письменном виде во время зачетной сессии. Для самостоятельной работы используются литературные источники, которые приведены в списке основной и дополнительной литературы по дисциплине.

Лабораторная работа проводится в компьютерном классе. Студенты получают задания, алгоритм выполнения работы, в конце занятия преподаватель проверяет проделанную работу.

В конце 4 семестра предусмотрен зачет, 5 семестра - экзамен.

8.2. Методические указания для студентов

Занятия проводятся в соответствии с учебным планом и расписанием, при этом на самостоятельную подготовку программой дисциплины отводится 75 часов. Данное время студенты планируют по индивидуальному плану, ориентируясь на перечень контрольных вопросов (п. 8.2.1.), заданий для самостоятельной работы (п. 8.2.2.) и список учебной литературы, рекомендуемый студентам в качестве основной и дополнительной по соответствующей дисциплине (п. 6.1.).

Для качественного освоения дисциплины «Информационная защита» студентам необходимо посещать лекционные и лабораторные занятия. Особое внимание следует уделить таким разделам, как «Правовые основы информационной безопасности личности, общества, государства, основные нормативно-правовые документы», «Методы и средства защиты информации».

На лекционных занятиях преподаватель в устной форме дает студентам основной материал раздела, студентам необходимо делать краткий конспект лекций. Во время аудиторных занятий преподаватель проверяет конспекты лекций студентов, студенты отвечают на вопросы для промежуточного контроля, решают практические задачи. Лабораторные работы проводятся в компьютерном классе. Студентам раздаются задания для самостоятельной работы, алгоритм выполнения. В конце изучения курса проводится контрольное тестирование, которое содержит 100 вопросов (критерий освоения дисциплины – 65 % правильных ответов). Формой итогового контроля в 4 семестре является зачет , 5 семестре - экзамен. Зачет и экзамен проводятся в виде устного опроса по билету, который содержит два вопроса. Время, которое отводится на подготовку к ответу, составляет 20 минут. Использование конспектов и учебников во время экзамена и зачета не допускается. При необходимости (спорная ситуация) экзаменатор может задавать студенту дополнительные вопросы. Помощь в подготовке к экзамену и зачету оказывает перечень примерных вопросов к экзамену и зачету, представленный в п. 8.2.4.

8.2.1. Перечень контрольных вопросов:

1. Информационное общество: общественный прогресс и новые реальности.
2. Информационная война.
3. Источники угроз ИБ РФ.
4. Информация. Право на информацию. Тайны.
5. Определение целей политики обеспечения информационной безопасности.
6. Международный обмен информации: проблемы свободы и ответственности.
7. Обзор зарубежного законодательства в области информационной безопасности.
8. О текущем состоянии российского законодательства в области информационной безопасности.
9. Угрозы безопасности информации и информационные атаки.
10. Защита информации и утечки по техническим каналам.
11. Интеллектуальная собственность в сети Интернет.
12. Как ломают телефонные сети.
13. Защита от подслушивания.

14. Защита от наблюдения и фотографирования.
15. Методы и средства защиты информации в мобильных системах.
16. Примеры отрицательных информационных влияний в обществе.
17. Необходимость различных форм контроля над информационными потоками в образовательном процессе.
18. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.
19. Определить объекты защиты авторских прав.
20. Назвать основные права автора в отношении его произведения.
21. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.
22. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).
23. Дать определение государственной тайны и назвать грифы секретности.
24. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.
25. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.
26. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.
27. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.
28. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.
29. Назвать основные виды служебной тайны определенные законодательством Российской Федерации.
30. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.
31. Назвать основные положения концепции информационной безопасности предприятия.
32. Изложить содержание регламента обеспечения информационной безопасности предприятия.
33. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.
34. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.
35. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.
36. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.
37. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.
38. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.
39. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.
40. Проанализировать особенности текста конфиденциального документа.
41. Проанализировать виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции.

8.2.2. Перечень тем заданий для самостоятельной работы:

4 семестр

1. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.
2. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.
3. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.
4. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.
5. Проанализировать пути поиска документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.
6. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.
7. Составить и проанализировать технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией.

5 семестр

1. Сформулировать возможности, трудности и направления использования электронной почты для передачи конфиденциальных документов.
2. Составить фрагмент номенклатуры дел, содержащих конфиденциальные документы.
3. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.
4. Ваша жизнь и информационные технологии? Назовите «плюсы» и «минусы».
5. Ваши интересы и психологическая безопасность под влиянием Интернета.

8.2.3. Перечень тем курсовых работ

1. Система информационной безопасности банка.
2. Источники возникновения и последствия реализации угроз информационной безопасности.
3. Основные проблемы информационной безопасности и методика их решения.
4. Экономическая безопасность деятельности фирмы.
5. Проектирование системы информационной безопасности.
6. Классификация и характеристика методов и средств защиты информации.
7. Компьютерные преступления и методы их защиты.
8. Технология защиты документной информации.
9. Ответственность за правонарушения в области защиты информации в России.
10. Защита авторских прав в интернете.
11. Информационная безопасность в зарубежных странах.
12. Основные направления деятельности службы безопасности предприятия (фирмы) по защите информационных ресурсов.
13. Компьютерные вирусы и механизм их действия.
14. Способы и средства защиты конфиденциальной информации техническими средствами.
15. Информационная безопасность человека.
16. Влияние средств массовой информации на человека.
17. Интернет и безопасность детей.

18. Информационные и психологические войны.

8.2.4. Перечень вопросов к зачету.

4 семестр

1. Понятие информации. Виды и свойства информации. Структура информационного процесса.
2. Окружающая среда как источник информации.
3. Роль информации в развитии общества.
4. Образование в информационном обществе.
5. Проблема «информационной безопасности».
6. Дайте определение «информационной безопасности».
7. Перечислите составляющие информационной безопасности и их определение.
8. Назовите взаимосвязь между составляющими информационной безопасности. Приведите собственные примеры.
9. Перечислите уровни формирования режима ИБ.
10. Правовые основы ИБ общества.
11. Ответственность за нарушения в сфере ИБ.
12. Стандарты ИБ: «Общие критерии».
13. Перечислите основные механизмы безопасности.
14. Назовите, что понимается под администрированием средств безопасности.
15. Содержание административного уровня обеспечения ИБ.
16. Дайте определение политики безопасности.
17. Перечислите классы угроз ИБ.
18. Назовите причины и источники случайных воздействий на информационные системы.
19. Дайте характеристику преднамеренным угрозам.
20. Перечислите каналы несанкционированного доступа.
21. Что понимается под техническим каналом утечки информации.
22. Охарактеризуйте угрозы доступности информации.
23. Основные угрозы целостности информации.
24. Понятие тайны, секрета, конфиденциальности.
25. Направления и методы защиты тайны в дореволюционной России и зарубежных странах.
26. Государственная тайна и системы ее защиты.
27. Служебная тайна.
28. Производственная тайна.
29. Профессиональная тайна.
30. Банковская тайна.
31. Тайны личная и семейная.
32. Институт тайн в законодательстве Российской Федерации.
33. Понятия – "фирменные секреты", "технологические секреты (ноу-хау)", "научные секреты (ноу-ноу)".
34. Понятие конфиденциальности как определение сферы несекретной информации ограниченного доступа.
35. Правовые и технологические аспекты присвоения информации категории конфиденциальной.
36. Конфиденциальная информация и ее виды. Общая классификация конфиденциальных документов.
37. Виды служб безопасности, их место в аппарате управления предпринимательских структур различных типов.
38. Защита информации при проведении совещаний и переговоров по конфиденциальным вопросам, приеме посетителей.

39. Угрозы безопасности информации от персонала и направления ее защиты.
40. Организация работы с персоналом, обладающим конфиденциальной информацией.
41. Понятие и задачи защищённого документооборота
42. Составляющие национальных интересов РФ в информационной сфере.
43. Основные направления и этапы работ по созданию комплексной системы безопасности предприятия (фирмы).
44. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков.

8.2.5. Перечень вопросов к экзамену.

5 семестр

1. Технические средства защиты информации.
2. Основы безопасности в Internet.
3. Электронная почта и ее защита.
4. Компьютерные вирусы и ИБ.
5. Назовите классификационные признаки и характерные черты компьютерных вирусов.
6. Перечислите деструктивные возможности компьютерных вирусов.
7. Перечислите виды «вирусоподобных» программ.
8. Поясните понятия «сканирование на лету» и «сканирование по запросу».
9. Перечислите виды антивирусных программ.
10. Охарактеризуйте антивирусные сканеры.
11. Назовите факторы, которые определяют качество антивирусных программ.
12. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
13. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
14. Основные понятия криптологии.
15. Требования к криптосистемам.
16. Основные алгоритмы шифрования.
17. Негативное воздействие рекламы на человека.
18. Информационная война.
19. Интеллектуальная собственность в сети Интернет.
20. Как ломают телефонные сети.
21. Защита от подслушивания.
22. Защита от наблюдения и фотографирования.
23. Методы и средства защиты информации в мобильных системах.
24. Сущность и современное состояние манипуляции сознанием и поведением людей.
25. Основные методы и средства информационного воздействия на человека.
26. Мифы как инструмент воздействия на людей.
27. Влияние средств массовой информации на мировоззрение людей и духовно-нравственное становление подрастающих поколений.
28. Повседневно-бытовой уровень манипуляции сознанием.
29. Защита русского языка – важное условие информационной безопасности России.
30. Глобальное общество и проблемы информационной безопасности.
31. Слухи как неформальный обмен информацией.
32. Информационные и психологические войны.
33. Влияние средств массовой информации на человека.
34. Методы тоталитарных сект и способы защиты от них.
35. Влияние рекламы на человека.
36. Влияние рекламы на детей.
37. Реклама нездорового образа жизни.
38. Интернет и безопасность детей.

39. Интернет-зависимость в подростковой среде.
40. Влияние жестоких компьютерных игр на поведение человека.

Программа составлена в соответствии с государственным образовательным стандартом высшего профессионального образования по направлению подготовки 050100.62 Естественнонаучное образование, профессионально-образовательный профиль Безопасность жизнедеятельности

Программу составили:

Доцент кафедры БЖД ТГПУ, к.ф-м.н. _____ У.М. Шеремetьева

Программа дисциплины утверждена на заседании кафедры «Безопасность жизнедеятельности»
протокол № 1 от «30» 08 2011 г.

Зав. кафедрой _____ А.С. Федотов

Программа дисциплины одобрена методической комиссией факультета технологии и предпринимательства ТГПУ

протокол № 1 от «31» 08 2011 г.

Председатель методической комиссии факультета
Технологии и предпринимательства _____ А.С. Федотов

Согласовано:
Декан факультета
Технологии и предпринимательства _____ Е.В. Колесникова

Лист внесения изменений в рабочую программу учебной дисциплины
ДПП.03 Информационная защита

Дополнения и изменения в рабочую программу учебной дисциплины на 2012/2013 учебный год.

В программу учебной дисциплины вносятся следующие изменения:

В пункт 8.2.1 «Перечень контрольных вопросов» добавляются следующие вопросы:

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности общества.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
10. Описать причины возникновения каналов несанкционированного доступа к информации.
11. Классифицировать виды каналов несанкционированного доступа к информации.
12. Описать характер действия организационных каналов несанкционированного доступа к информации.
13. Охарактеризовать технические каналы несанкционированного доступа к информации.
14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.
15. Проанализировать особенности угроз автоматизированным информационным системам.
16. Дать классификацию удаленных атак.
17. Проанализировать основные направления правовой защиты информации.
18. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.
19. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.
20. Назвать основные элементы физической защиты территории и помещений предприятия.
21. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов.
22. Дать классификацию компьютерных вирусов.
23. Описать основные антивирусные программы.
24. Охарактеризовать основные способы криптографического преобразования данных.
25. Почему тысячелетиями людям не удается создать оптимальное для жизни общественное устройство?
26. Что вы слышали о движении «антиглобалистов», как к нему относитесь?
27. Что такое «золотой миллиард», кто определяет, по каким критериям люди входят в него?
28. Чем опасно нивелирование под единый стандарт информационных систем всех людей и стран?

29. Какова роль духовности в обеспечении безопасности человека и всего общества?
30. Почему некоторые заболевания называются «болезнями цивилизации»? Что это за болезни?
31. Считаете ли вы свое поведение «зависимым»? В каких формах эта зависимость проявляется и каковы ее признаки?
32. Как вы относитесь к законодательному и практическому ограничению возможностей игрового бизнеса?
33. Что делать, если в беду попал близкий человек?
34. В чем смысл известного утверждения древних: «Хочешь вылечить тело – лечи душу»?
35. Почему отечественные товары рекламируются меньше и не столь красочно, как западные?
36. Есть ли различия в отношении к рекламе учащихся и их родителей?
37. Визуальная реклама на зданиях и улицах украшает город или портит его внешний вид?
38. Есть ли у вас свои варианты использования рекламной продукции (или рекламных пауз) не по ее предназначению, но с пользой для здоровья, познания или времяпрепровождения?

Изменения в рабочую программу внесены:

Доцент кафедры БЖД, к.ф.-м.н. _____ У.М. Шереметьева

Изменения в рабочую программу учебной дисциплины утверждены на заседании кафедры «Безопасность жизнедеятельности»

протокол № 1 от «30» 08 2012 г.

Зав. кафедрой _____ А.С. Федотов

Изменения в рабочую программу учебной дисциплины одобрены методической комиссией факультета технологии и предпринимательства ТГПУ

протокол № 1 от «31» 08 2012 г.

Председатель методической комиссии факультета
Технологии и предпринимательства _____ А.С. Федотов

Согласовано:

Декан факультета
технологии и предпринимательства _____ Е.В. Колесникова