МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

Институт систем управления

Кафедра прикладной информатики и информационной безопасности

АННОТАЦИЯ

по дисциплине

«Компьютерная экспертиза»

направление подготовки 10.03.01 Информационная безопасность

профиль «Организация и технология защиты информации»

очной формы обучения

Соответствует РПД

УМУ СГЭУ

Зав. кафедрой _____

/Абросимов А.Г./

Самара 2015 г.

1. Цели и задачи изучения дисциплины

Целью дисциплины «Компьютерная экспертиза» является формирование у студентов знаний по основам защиты информации, а также навыков и умения в применении знаний для конкретных условий.

Задачами дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

2. Место дисциплины в структуре ООП:

Дисциплина “Комплексная система зашиты информации на предприятии” относится к разделу Б3.В.ОД.3, входит в вариативную часть профессионального цикла, читается студентам в 7 и 8 семестрах.

Для освоения курса студентам необходимо предварительно овладеть знаниями и умениями по дисциплинам:

- Информатика
- Теория информации
- Основы информационной безопасности
- Информационные технологии
- Теория систем и системный анализ
- Физические основы защиты информации
- Мировые информационные ресурсы
- Аппаратные средства вычислительной техники
- Программно-аппаратные средства защиты информации
- Криптографические методы защиты информации
- Языки программирования
- Технологии и методы программирования
- Техническая защита информации
- Комплексные системы защиты информации на предприятии.

Знания, полученные при изучении данной дисциплины, необходимы в дипломном проектировании.

3. Требования к уровню подготовки студента

Процесс изучения дисциплины «Компьютерная экспертиза» направлен на формирование следующих компетенций:

ПК-6	способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов
ПК-14	способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности
ПК-21	способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов

В результате изучения дисциплины студенты должны:

иметь представление:

- о задачах, структуре и возможностях технической разведки, основных этапах и процессах извлечения информации;
- о физических процессах в технических средствах и системах, способствующих утечке защищаемой информации;
- о характеристиках используемых и перспективных технических средств добывания и защиты информации;
- о государственной системе защиты информации и ее основных документах;

знать:

- виды, источники и носители защищаемой информации;
- основные угрозы безопасности информации;
- концепцию инженерно-технической защиты информации;
- основные принципы и методы защиты информации;
- основные руководящие и нормативные документы по инженерно-технической защите информации;
- порядок организации инженерно-технической защиты информации;

уметь:

- выявлять угрозы и технические каналы утечки информации;
- описывать (моделировать) объекты защиты и угрозы безопасности информации;
- применять наиболее эффективные методы и средства инженерно-технической защиты информации;
- контролировать эффективность мер защиты;

иметь навыки:

- аппаратурной оценки энергетических параметров побочных излучений от технических средств и систем;
- инженерного расчета уровня защиты контролируемой зоны.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетные единицы.

Вид учебной работы	**Всего часов/зачетных единиц** **УП 2012 -8 семестр**	**Всего часов/зачетных единиц** **УП 2013 -7 семестр**
Аудиторные занятия	48 / 1,33	54 / 1,5
В том числе:		
Лекции	16/0,44	18/0,5

Практические занятия	32 /0,89	36 / 1
Самостоятельная работа (всего)	24 / 0,67	18 / 0,5
В том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Реферат		
Другие виды самостоятельной работы		
Вид промежуточной аттестации (зачет, экзамен)	зачет	зачет
Общая трудоемкость	72/2	72 /2

Содержание аудиторных занятий

Наименование других дисциплин и их разделов, используемых при изучении данной дисциплины	ЛЕКЦИОННЫЕ ЗАНЯТИЯ		Наименование других дисциплин и их разделов, использующих знания, полученные изучении данной дисциплины	
	Номер, наименование темы и раздела. Содержание раздела.	Объем в часах	Практические работы	Объем в часах
1	2	3	4	5
	Раздел 1. Компьютерные преступления Криминалистическая характеристика. Личность вероятного преступника. Оперативность Приоритетность расследования. Онлайн-мошенничество. Преступник. Потерпевший. Следы.	2		4
	Раздел 2 **Оперативно-розыскные мероприятия** 2.1. Взаимодействие. Перехват и исследование трафика. Исследование статистики трафика. Другие данные о трафике. Анализ заголовков пакетов. Исследование системных логов Системные логи Windows. 2.2. Документирование прохождения сообщений. Анонимные ремейлеры. Установление принадлежности и расположения IP-адреса. Установление принадлежности доменного имени. Принадлежность адреса электронной почты	4		6
	Раздел 3. **Следственные действия** 3.1. Осмотр компьютера Особенности. Стандарты. Лог-файлы, доказательная сила лог-файлов. Лог как доказательство. Цепочка доказательности. Корректность изъятия. Неизменность после изъятия. Процедура приобщения логов. 3.2. Тактика обыска. Общие правила изъятия компьютер-	4	Практическая работа	6

	ной техники при обыске. Особенности. Ноутбук (лэптоп, переносной компьютер). Принтеры. Сканеры. Флэш-накопители. Мобильные телефоны.			
	Раздел 4. **Компьютерно-техническая экспертиза** 4.1. Место и роль КТЭ. Кто может быть экспертом? Поиск информации. Следы. Программы. Время. Оценка содержания. Объекты исследования. 4.2. Методы КТЭ. Исследование файловых систем. Копирование носителей. Исследование файлов. Другие типы носителей. Флэш-накопители. Неаккуратное обращение с паролем. Экспертные инструменты и авторское право. Поиск информации на диске. Информация о файлах. Подключение образа диска. Изучение архивов электронной почты и ICQ	4	Практическая работа	14
	Раздел 5. **Участие специалиста в судебном заседании** 5.1.	2	Практическая работа	2
Итого в 8 семестре		**16**		**32**

Текущий и промежуточный контроль знаний студентов

Наименование контрольного мероприятия	Наименование раздела (темы) дисциплины	Срок проведения (неделя семестра или номер занятия)	Форма оценивания результата и дополнительные сведения (балльная оценка, допуск/ недопуск, % выполнения и т.п.)
1	2	3	4

Контрольный опрос	Раздел 1-3	6	Балльная оценка
Контрольный опрос	Раздел 4	10	Балльная оценка

Технические средства и материальное обеспечение учебного процесса

Учебно-методическое обеспечение

Основная литература:

- Вехов В.Б., Илюшин Д.А., Попова В.В. Тактические особенности расследования преступлений в сфере компьютерной информации: Научно-практическое пособие. 2-е изд. - М.: ЛексЭст, 2004.
- Завидов Б.Д. Обычное мошенничество и мошенничество в сфере высоких технологий. М., 2002.
- Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. Воронеж, 2001.
- Крылов В.В. Расследование преступлений в сфере информации. - М.: Городец, 1998.
- Экспертизы на предварительном следствии: Краткий справочник / Под общ. ред. В.В.Мозякова. - М.: ГУ ЭКЦ МВД России, 2002.
- Горбатов В.С., Полянская О.Ю. Мировая практика криминализации компьютерных правонарушений. - М.: МИФИ, 1996.
- Губанов В.А., Салтевский М.В., Щербаковский М.Г. Осмотр компьютерных средств на месте происшествия: Методические рекомендации. - Харьков: Академия правовых наук Украины, НИИ изучения проблем преступности, 1999.
- Михайлов И.Ю. Методические рекомендации: Носители цифровой информации (обнаружение, изъятие, назначение компьютерно-технической экспертизы). - Курган: ЭКЦ при УВД Курганской области, 2003.

Дополнительная литература:

- Почепцов Г.Г. Информационные войны. - М.: Рефл-бук, К., Ваклер, 2000.
- Панарин И. Технология информационной войны. Издательство «КСП+», 2003.
- Соловьев Л.Н. Классификация способов совершения преступлений, связанных с использованием и распространением вредоносных программ для ЭВМ.
- Иванов Н.А. Применение специальных познаний при проверке «цифрового алиби» // журнал «Информационное право», 2006. №4 (7).
- Середа С.А., Федотов Н.Н. Ответственность за распространение вредоносных программ для ЭВМ // Право и экономика. 2007, №3. С. 50-55.
- Компьютерное пиратство: методы и средства борьбы: Методическое пособие. 8-е изд. - М.: НП ППП, 2005.

Электронные источники и интернет-ресурсы

- Пятиизбянцев Н. Проблемы уголовно-правовой борьбы с преступлениями в области банковских карт. http://bankir.ru/analytics/Ur/36/66441
- Безмалый В.Ф. Мошенничество в Интернете // «Security Lab», 6 декабря 2006. http://www.securitylab.ru/contest/280761.php
- Собецкий И.В. Организация технико-криминалистической экспертизы компьютерных систем // «Security Lab», 10 ноября 2003. http://www.securitylab.ru/analytics/216313.php
- Техника для спецслужб Технические средства защиты информации [http://www.t-ss.ru/baron.htm].
- ООО «Защита информации» [http://www.zinfo.ru/item/859/]

Нормативные акты

- Постановление Правительства РФ от 27 августа 2005 г. №538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность» // Собрание законодательства Российской Федерации, №36, 05.09.2005, ст. 3704.
- Постановление Пленума Верховного Суда Российской Федерации №15 от 19 июня 2006 г. «О вопросах, возникших у судов при рассмотрении гражданских дел, связанных с применением законодательства об авторском праве и смежных правах».
- Правила регистрации доменных имен в домене RU - нормативный документ Координационного центра национального домена сети Интернет, утвержден решением П2-2.1, 4.1/06 от 24.04.2006.
- Федеральный закон «Об оценочной деятельности в Российской Федерации» от 29 июля 1998 г. (№135-ФЗ).
- Закон РФ «О коммерческой тайне» (№98-ФЗ).

Методические указания и рекомендации

Примерная программа обеспечивает реализацию системного подхода к образовательному процессу. Он предусматривает:

- представление знаний по дисциплине в виде иерархической структуры (пирамиды), каждый уровень которой соответствует определенному уровню обобщения знаний: концепция инженерно-технической защиты, теория, физика, техника, организация, методика. Последовательность изложения соответствует конкретизации знаний, рассмотренных на предыдущем уровне;
- лабораторные и практические работы объединены в единый цикл работ по единым разрабатываемым преподавателем сценариям, предусматривающих решение практических задач по обеспечению

информационной безопасности на объекте защиты (помещении, здании, организации).