

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение высшего профессионального образования
«Уральский государственный университет им. А.М. Горького»

ИОНЦ «Информационная безопасность»
математико-механический факультет
кафедра алгебры и дискретной математики

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ

**Противодействие созданию и распространению
вредоносных программ**

Рабочая программа дисциплины

Автор: доцент кафедры алгебры
алгебры и дискретной математики
В.В. Бакланов

Екатеринбург
2008

Министерство образования и науки Российской Федерации
Федеральное агентство по образованию
ГОУ ВПО «Уральский государственный университет»

УТВЕРЖДАЮ

Проректор университета

_____._____. 2007 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Противодействие созданию и распространению вредоносных программ

Рекомендована Методическим советом УРГУ
для специальности 090102 – Компьютерная безопасность

Екатеринбург 2008

Рабочая программа составлена на основании Государственного образовательного стандарта высшего профессионального образования, утвержденного приказом Министерства образования Российской Федерации № 686 от 2 марта 2000 года.

Программу составил: доцент, к.т.н. Бакланов В.В.

Рабочая программа одобрена на заседании кафедры алгебры и дискретной математики « ____ » _____ 2008 г., протокол № ____.

Заведующий кафедрой
профессор, д.ф-м.н. _____ *Волков М.В.*

Рабочая программа одобрена на заседании Методической комиссии математико-механического факультета
« ____ » _____ 2008 г., протокол № ____

Председатель методической комиссии _____

АННОТАЦИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

Дисциплина посвящена изучению организационных, технологических и программно-аппаратных мер защиты от опасной компьютерной информации, в первую очередь – от вредоносных программ для ЭВМ. Деятельность по созданию и распространению программ для ЭВМ рассматривается как рискованная и потенциально опасная. Рассматриваются виды опасных программ, команд и данных. Дается развернутая классификация опасных последствий запуска вредоносных программ в формах несанкционированного удаления, копирования, блокирования и модификации компьютерной информации, нарушения работы ЭВМ. Изучаются особенности построения и функционирования компьютерных вирусов, программных закладок, сетевых вредоносных программ и др. Подробно рассматриваются приемы и способы несанкционированного распространения, внедрения и запуска вредоносных программ. Изучаются методы и технология антивирусной защиты. Излагаются приемы и способы криминалистического исследования потенциально опасных программ.

Дисциплина опирается на ранее изученные дисциплины «Организационно-правовое обеспечение информационной безопасности», «Безопасность операционных систем», «Программно-аппаратные средства обеспечения информационной безопасности».

1. Цели и задачи дисциплины

Целью дисциплины «Противодействие созданию и распространению вредоносных программ» является формирование у студентов знаний и представлений о смысле, целях и задачах защиты от различных видов опасной компьютерной информации, включая вредоносные программы.

Приобретенные знания позволят студентам правильно строить систему антивирусной безопасности организации и учреждения, а также выступать в роли частного эксперта или специалиста при расследовании компьютерных преступлений.

2. Требования к уровню освоения дисциплины

В результате изучения дисциплины студенты должны

2.1 Знать:

- основные причины и особенности современных информационных и компьютерных преступлений;
- составы преступлений в сфере компьютерной информации, предусмотренные УК РФ, и толкование специальных терминов, употребляемых в них;
- современные возможности криминалистического исследования машинных носителей информации, программного обеспечения и компьютерных данных;
- возможности и отличительные признаки различных видов вредоносных программ для ЭВМ;
- порядок применения антивирусного программного обеспечения;
- принципы исследования потенциально опасных программ для ЭВМ;
- порядок поиска и юридического закрепления доказательной компьютерной информации;
- нормативные требования о порядке проведения процессуальных действий и компьютерно-технических экспертиз;
- права и обязанности специалиста и эксперта;
- требования к составлению итоговых заключений специалиста и эксперта в сфере компьютерных технологий.

2.2 Уметь:

- фиксировать при проведении следственных действий криминалистически значимую компьютерную информацию, в том числе осуществлять ее копирование;
- самостоятельно проводить простые диагностические экспертизы и исследования в сфере компьютерных технологий;
- проводить криминалистические осмотры компьютерной аппаратуры, оборудования, данных и программного обеспечения;
- искать, восстанавливать и сохранять доказательную компьютерную информацию;

- определять признаки вредоносности компьютерных программ,
- обнаруживать присутствие вредоносного программного кода в статическом и динамическом режимах,
- правильно применять средства антивирусной защиты отечественных и зарубежных производителей,
- использовать эвристические методы и алгоритмы защиты от вредоносных программ.

3. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестры	
			10
Общая трудоемкость дисциплины	100		
Аудиторные занятия	36		
Лекции (Л)	12		12
Лабораторные работы (ЛР)	24		24
Самостоятельная работа (СР)	32		32
Курсовая работа	24		24
Вид итогового контроля (зачет, экзамен)			Экзамен

4. Содержание дисциплины

4.1. Информационные и компьютерные преступления

Понятие об информационных и компьютерных преступлениях. Особенности и причины информационных преступлений. Понятие о неправомерном обороте информации. Составы информационных преступлений, предусмотренные Уголовным кодексом РФ. Преступления в форме незаконного распространения, разглашения и передачи информации. Незаконное воспрепятствование доступу к информации. Незаконное хранение и использование конфиденциальной информации. Формы информационной фальсификации. Компьютерные мошенничества.

Особенности компьютерных преступлений. Преступления в сфере компьютерной информации. Место компьютерных систем в преступной деятельности. Компьютер как непосредственное орудие преступления. Компьютер как средство преступления и хранилище информации о преступной деятельности. Компьютер как предмет преступления. Особенности подготовки компьютерных преступлений.

Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Характеристика объективной стороны преступлений, предусмотренных гл. 28 УК РФ. Виды ЭВМ по отношению к преступной деятельности. Способы нарушения работы ЭВМ, системы ЭВМ и их сети. Формы несанкционированного копирования, удаления, модификации и блокирования защищаемой законом компьютерной информации. Ответственность за совершение преступлений, предусмотренных ст. 272 – 274 УК РФ.

4.2. Понятие об опасной компьютерной информации

Создание и использование компьютерных программ как деятельность, представляющая повышенную общественную опасность. Уровни представления опасной компьютерной информации. Понятие компьютерных программ и команд. Программы и данные как объективная форма представления компьютерной информации. Машинный код. Ассемблерные команды. Опасные системные вызовы. Опасные системные команды. Инструментарий для разработки, отладки и модификации вредоносных программ.

4.3. Классификация и технические возможности вредоносных программ.

Понятие о вредоносных программах. Классификация вредоносных программ по основным свойствам и признакам. Классификация программ по степени опасности для защищаемой информации и компьютерной системы. Деструктивные функции вредоносных программ. Механизмы вирусного заражения. Способы выявления деструктивной активности программ. Понятие о сигнатуре вредоносного программного кода. Принцип антивирусного сканирования. Антивирусные сканеры, мониторы и сетевые фильтры.

4.4. Уязвимые места программного обеспечения ЭВМ, способствующие внедрению, сокрытию, распространению и запуску вредоносных программ.

Потенциально опасные функции и элементы операционной системы. Возможности использования уязвимостей ОС и штатного программного обеспечения с целью удаления, модификации, блокирования или копирования информации без уведомления и согласия ее владельца или пользователя. Понятие о случайном или безусловном запуске. Способы подготовки вредоносных программ к автоматическому запуску. Типичные варианты обмана пользователей, провоцирующих их на запуск неизвестных программ. Понятие о механизмах скрытности вредоносных программ. Полиморфизм программного кода. «Stealth»-технологии. Иные способы сокрытия. Уязвимости ОС и штатного программного обеспечения, позволяющие вредоносным программам самопроизвольно распространяться на машинных носителях и по компьютерной сети.

Защита компьютерных систем от вредоносного программного воздействия. Понятие об опасных и вредоносных программах. Характеристика компьютерной программы как вида информационного нарушителя. Классификация вредоносных программ. Демаскирующие признаки опасного программного воздействия. Основные организационные и программные меры антивирусной защиты.

4.5. Изучение функциональных возможностей вредоносных программ.

Основные признаки и возможности макровирусов, сетевых «червей», программ «удаленного администрирования». Способы проникновения вредоносных программ в локальные и сетевые ЭВМ.

Способы выявления деструктивной активности вредоносных программ. Понятие о сигнатуре вредоносного программного кода. Принцип антивирусного сканирования. Понятие о механизмах скрытности вредоносных программ.

Демаскирующие признаки вредоносного программного кода. Полиморфизм программного кода. Программы-«невидимки». Способы сокрытия файловых объектов и процессов на уровне ядра операционной системы. Возможности программ-«руткитов». Мониторинг подозрительной активности программ. Виды и возможности антивирусных программ. Статическое и динамическое исследование подозрительных программ. Организационные и технические меры по обеспечению изоляции программной среды.

Изучение функциональных возможностей вредоносных программ. Статический анализ потенциально опасных программ. Определение истинного типа файла. Просмотр текстовых строк в исполняемых и командных файлах. Рекомендации по дизассемблированию и исследованию программного кода. Динамический анализ опасных программ. Запуск программ в виртуальной среде VMWare. Трассировка программ. Возможности программ типа ExeScore и OllyDebugger. Использование мониторов обращений к стеку сетевых драйверов, файлам и системному реестру. Оформление заключений по результатам исследования неизвестных и опасных программ.

5. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Таблица 5.1 – Распределение лабораторных работ по разделам дисциплины

№ работы	Наименование работы	Время на выполнение работы, час
1	Исследование деструктивных возможностей потенциально опасных программ и команд	4
2	Исследование возможностей скрытого внедрения и запуска опасных программ	4
3	Исследование интерпретируемых вредоносных программ (командных файлов, макросов и сценариев)	4
4	Исследование кооперативных вирусов	4
5	Исследование защитных механизмов Microsoft Word	4
6	Исследование защитных механизмов Microsoft Internet Explorer	4

6. Учебно-методическое обеспечение дисциплины

6.1. Нормативно-правовые акты

1. Конституция РФ от 12.12.93 (с изм. и доп. от 10.02.1996).
2. Уголовный кодекс Российской Федерации № 63-ФЗ от 13.06.1996 (с изм. и доп. от 07.07.2007).
3. Уголовно-процессуальный кодекс Российской Федерации № 174-ФЗ от 18.12.2001 (с изм. и доп. от 07.07.2003).
4. Кодекс РФ об административных нарушениях № 195-ФЗ от 30.12.2001 (с изм. и доп. от 4.07.2003).
5. Гражданский кодекс РФ. Часть четвертая. ТК Велби, Изд-во Проспект, 2007. 176 с.
6. ФЗ «Об информации, информационных технологиях и защите информации», № 149-ФЗ от 27.07.2006.
7. ФЗ «О персональных данных», № 152-ФЗ от 27.07.2006.
8. ФЗ «О связи», № 126-ФЗ от 07.07.2003.

6.2. Основная литература

1. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер. с англ. / Дэвид Айков, Карл Сейгер, Уильям Фонсторх. – М.: Мир, 1999. – 351 с.
2. Бакланов В.В. Опасная компьютерная информация / В.В.Бакланов. Екатеринбург, в/ч 69617. 2006. 123 с.
3. Вехов В. Б. Тактические особенности расследования преступлений в сфере компьютерной информации: научно-практ. пособие – 2-е изд., доп. и испр. / В. Б. Вехов, В. В. Попова, Д. А. Илюшин. – М.: ЛексЭст, 2004. – 160 с.
4. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз. – М.: ООО Издательство Юрлитинформ, 2002. – 496 с.
5. Гаврилин Ю. В. Преступления в сфере компьютерной информации: квалификация и доказывание : учеб. пособие / Ю. В. Гаврилин, А. В. Кузнецов, А. Ю. Головин, Т. В. Толстухина, А. В. Кузнецов. – М.: ЮИ МВД РФ, 2003. – 245 с.
6. Кэрриэ Б. Криминалистический анализ файловых систем: Пер. с англ. / Б. Кэрриэ. – СПб.: Питер, 2007. – 480 с.
7. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / В. Е. Козлов. – М.: Горячая линия – Телеком, 2002. – 336 с.
8. Мазуров В. А. Компьютерные преступления: классификация и способы противодействия: учеб. – практическое пособие / В. А. Мазуров. – М.: Палеонтип, Логос, 2002. – 148 с.

9. Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры Пер. с англ. / Д. Макнамара. – М.: БИНОМ. Лаборатория знаний, 2004. – 536 с.
10. Мандиа К. Защита от вторжений. Расследование компьютерных преступлений: Пер. с англ. / К. Мандиа, К. Просис. – М.: ЛОРИ, 2005. – 476 с.
11. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография / А. Л. Осипенко. – М.: Норма, 2004. – 432 с.
12. Соловьев Л. Н. Вредоносные программы: расследование и предупреждение преступлений / Л. Н. Соловьев. – М.: Собрание, 2004. – 224 с.
13. Усов А. И. Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: учеб. пособие / А. И. Усов. – М.: Изд-во Экзамен, Право и закон, 2003. – 368 с.
14. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998. – 288 с., ил.
15. Касперский К. Техника и философия хакерских атак. - М.: «Солон - Р», 1999, 272с.
16. Крис Касперски. Укрощение Интернета. –М.: СОЛОН-Р, 2002. –288 с.
17. Скэмбрей Джоел, Мак-Клар Стюарт. Секреты хакеров. Безопасность Windows 2000 – готовые решения. Пер. с англ. –М.: Издательский дом «Вильямс», 2002. –464 с.
18. Стюарт Мак-Клар, Джоел Скембрей, Джордж Курц. Секреты хакеров. Безопасность сетей - готовые решения, 2-е изд.: Пер. с англ. - М.: Издательский дом "Вильямс", 2001. -656 с.

6.3. Дополнительная литература:

1. Крылов В. В. Информационные компьютерные преступления / В. В. Крылов. – М.: ИНФРА-М-НОРМА, 1997. – 285 с.
2. Курушин В. Д. Компьютерные преступления и информационная безопасность: справочник / В. Д. Курушин, В. А. Минаев. – М.: Новый Юрист, 1998. – 256 с.
3. Леонтьев Б. Хакеры, взломщики и другие информационные убийцы / Б. Леонтьев. – М.: Познавательная книга, 1999. – 192 с.
4. Медведовский И. Д. Атака на Internet: – 2-е изд., перераб. и доп. / И. Д. Медведовский, П. В. Семьянов, Д. Г. Леонов. – М.: ДМК, 1999. – 336 с.
5. Гульев И. Компьютерные вирусы, взгляд изнутри — М.: ДМК, 1998 — 304 с.
6. Таненбаум Э. Современные операционные системы. 2-е изд. -СПб.: Питер, 2002. -1040 с.
7. Хоникатт Джерри. Реестр Windows 2000. Пер. с англ. Уч. пос. –М.: Издательский дом «Вильямс», 2000. –320 с.

7.1. Средства обеспечения освоения дисциплины

В процессе изучения дисциплины используются:

- компьютерные презентации, разработанные в среде Microsoft PowerPoint;
- учебный материал в электронном виде.

7.2. Общие требования

Лекционный материал должен изучаться в специализированной аудитории, оснащенной современным компьютером и проектором с видеотерминала персонального компьютера на настенный экран.

Лабораторные работы должны проводиться в условиях специализированного компьютерного класса, оборудованного персональными ЭВМ. Минимальные технические требования к персональным компьютерам: платформа IA-32, тактовая частота центрального процессора не ниже 2 ГГц, оперативная память объемом не менее 512 Мбайт, два жестких магнитных диска емкостью не менее 100 Гбайт каждый с интерфейсами IDE или Serial ATA, и устройством Mobile Rack.

Требования по обеспечению информационной безопасности: при проведении лабораторных работ: все компьютеры должны быть изолированы от локальной вычислительной сети (путем извлечения разъема сетевого кабеля из адаптера). Для исследования возможностей вредоносных программ могут использоваться только съемные жесткие магнитные диски, на которых размещаются загружаемые операционные системы, утилиты для исследования опасного программного кода, фрагменты исследуемых вредоносных программ и антивирусное программное обеспечение. Для исследования возможностей макровирусов на диски устанавливается офисное приложение Microsoft Word версий 10.0-12.0. При проведении работ с целью недопущения копирования обучаемыми кодов вредоносных программ приводы ГМД, CD/DVD-RW, проводные интерфейсы USB и IEEE 1394 отключаются в настройках Setup BIOS.

8.1. Перечень контрольных вопросов для подготовки к итоговой аттестации по дисциплине

1. Формы и особенности представления компьютерной информации.
2. Понятия об информационных и компьютерных преступлениях.
3. Основные причины и особенности компьютерных преступлений.
4. Компьютерная система как орудие преступления.
5. Компьютерная система как средство совершения преступления и хранилище информации о преступной деятельности.
6. Вредоносный программный код документов офисных приложений и его возможности. Методы вирусного копирования.
7. Реализация защиты от вредоносного программного кода в приложениях офисного пакета. Нейтрализация вредоносных макросов с целью их исследования.
8. Механизм сетевых атак на Интернет-браузеры (на примере Microsoft Internet Explorer). Механизмы статического скрывания вредоносного программного кода.

9. Механизмы скрытности вредоносных программ на этапе их выполнения.
10. Механизмы скрытия, используемые современными макровирусами.
11. Классификация и основные особенности различных видов вредоносных программ.
12. Способы подготовки вредоносных программ к безусловному запуску. Несанкционированный характер запуска вредоносных программ.
13. Внедрение и запуск вредоносных программ на этапах самотестирования компьютера и загрузки операционной системы. Способы автоматического запуска вредоносных программ.
14. Возможности программных закладок. Виды и способы программного перехвата компьютерной информации.
15. Виды компьютерных инфекций. Сущность вирусного заражения и жизненный цикл компьютерного вируса.
16. Возможности и особенности сетевых вредоносных программ.
17. Понятие о «тройанских» программах и их функциях. Программы-«джойнеры».
18. Виды несанкционированного копирования компьютерной информации.
19. Виды нарушений работы ЭВМ со стороны вредоносных программ.
20. Виды несанкционированного блокирования и модификации компьютерной информации вредоносными программами.
21. Традиционные способы антивирусной защиты и сравнительная оценка их эффективности.
22. Требования к экспертному заключению.
23. Порядок поиска доказательной информации в памяти ЭВМ.