

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

**Противодействие созданию и распространению
вредоносных программ**

Методические указания по изучению дисциплины

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

Екатеринбург
2008

Существует особая категория программистов, именуемых вирусописателями или вирмейкерами. Представители этой, не такой уж и маленькой группы людей, порознь или сообща, часто без какой-либо материальной выгоды для себя, а зачастую с риском быть привлеченными к уголовной ответственности, пишут заведомо вредоносные программы для ЭВМ. Цели подобной деятельности различны — от любопытства начинающего программиста до стремления причинить вред всем и каждому. Компьютер позволяет таким людям, часто неудачливым и несчастливым в обычной жизни, ощутить свое превосходство над окружающими и получать извращенное наслаждение от власти над простыми пользователями.

Цель изучения дисциплины «Противодействие созданию и распространению вредоносных программ» заключена в ее названии. Именно создание и распространение вредоносных программ являются наиболее опасными формами преступного деяния, предусмотренного статьей 273 УК РФ. К нашему великому сожалению, эта деятельность набрала уже такой размах, что победить ее кажется невозможным. Но противодействовать этому можно и должно.

Существует довольно много видов компьютерных программ, которые потенциально опасны для обрабатываемой информации, но их создание, распространение и использование не подпадает под юрисдикцию Уголовного кодекса. Множество вполне безобидных компьютерных программ находят применение в различных видах преступной деятельности. Так, обычный текстовый редактор может использоваться для написания листовки, призывающей к свержению конституционного строя, а компьютерный тренажер являться средством подготовки к совершению террористического акта. Но опасная компьютерная информация не исчерпывается одними программами. Наряду с ними опасными могут стать системные данные, а иногда — даже пользовательские данные. Поэтому одно из учебных пособий вполне обосновано называется «Опасная компьютерная информация».

Дисциплина в методическом отношении прикрывается двумя учебными пособиями: «Опасная компьютерная информация» и «Защита компьютерной информации в клиентских приложениях». Все лекции обеспечены компьютерными презентациями Microsoft PowerPoint. Большое внимание уделено практическому закреплению изучаемого материала с элементами учебной исследовательской деятельности. Программой дисциплины предусмотрено шесть лабораторных работ продолжительностью 4 часа каждая.

При изложении дисциплины автор преследует несколько целей. Во-первых, дать более полную и правильную классификацию вредоносных программ, причем более четко выделить их функциональные особенности. Во-вторых, создать представление о конкретных опасных последствиях, «разложив» их по пространству объективной стороны преступлений в сфере компьютерной информации. В-третьих, уделить внимание изучению механизмов, которые позволяют вредоносным программам внедряться в компьютерные системы, получать возможности для запуска на исполнение и скрываться от глаз пользователя и антивирусных программ. Наконец, особое

внимание уделено рассмотрению действий вредоносных программ, заведомо приводящих к общественно опасным последствиям, предусмотренным ст. 273 УК РФ. В тексте учебных пособий, обеспечивающих дисциплину, приведены многочисленные примеры опасных команд, вызова опасных функций и фрагментов вредоносных программ. Сделано это вовсе не с целью обучения кого бы то ни было вредоносному программированию, а исключительно из понимания того, что победить вооруженного противника, досконально не изучив его вооружения, нельзя. Задача состоит не в том, чтобы научиться писать вредоносные программы, а в том, чтобы наглядно представлять себе и степень их реальной опасности, и условия, в которых они могут создаваться. Две лабораторные работы связаны с исследованием статического кода реальных вредоносных программ, алгоритм которых необходимо понять и изложить в виде комментариев. Для образца предлагается одно из собственных авторских экспертных исследований.

Учебная дисциплина не ограничивается рассмотрением только опасных компьютерных программ. Изучению подлежит и методология опасного интерактивного управления компьютером, и управляющие данные, и данные, обработка которых может причинить ущерб защищаемой компьютерной информации и компьютерной системе. Вредоносная программа часто является лишь фитилем у бочки с порохом, каким является операционная система.

Защита компьютерной информации с позиций администратора безопасности привычно ассоциируется именно с операционной системой. Действительно, большинство защитных механизмов, от разграничения доступа пользователей к файлам до шифрования данных, размещено именно в операционной системе. Вместе с тем определенная часть задач по защите компьютерной информации ложится на программные приложения, с которыми приходится работать пользователю. Это средства создания и редактирования текстовых документов, электронные таблицы, системы управления базами данных, почтовые клиентские программы и Интернет-браузеры. Так, для операционной системы Windows* документ Word – это просто файл, который она распознает только по характерному расширению .doc. Опасные функции, содержащиеся в этом документе, в том числе потенциально опасный программный код, видны только его «родной» программе – текстовому процессору Word (для которого, кстати сказать, расширение имени файла .doc не является значимой информацией). На уровне приложения определяется и механизм шифрования конфиденциального документа, и стратегия резервирования и восстановления содержимого файлов на случай сбоя, и защита от вредоносных программ в макросах.

От браузера, с помощью которого осуществляется получение информации в Интернет, зависит не только производительность поиска и отображения этой информации, но и защита всей компьютерной системы от сетевых атак и проникновения вредоносных программных компонентов. Большинство программных приложений в отношении обрабатываемой информации выполняют роль самостоятельных операционных систем.

Во втором учебном пособии рассматривается защита компьютерной информации в клиентских приложениях, и в качестве примеров рассматриваются две весьма примечательные программы (точнее не программы, а целые программные пакеты), разработанные в фирме Microsoft, – текстовый процессор Word и браузер Internet Explorer. В настоящее время опубликовано много книг по защите серверов, предоставляющих услуги сети Интернет. Защита серверов безусловно важна, но следует признать, что пользователей в компьютерном мире гораздо больше, и от их безопасности в первую очередь зависит компьютерная безопасность общества в целом.

В теоретической части каждой темы излагаются способы и средства защиты информации, реализованные в рассматриваемых приложениях, а также типичные компьютерные атаки, которые когда-либо были успешно проведены информационными злоумышленниками по причине уязвимостей, допущенных программистами фирмы Microsoft. Теоретический материал дополняется лабораторным практикумом, позволяющим обучаемым самостоятельно исследовать некоторые уязвимости и защитные механизмы прикладных программ.

Современные уязвимости программных приложений Microsoft Word и Microsoft Internet Explorer, обнаруженные рядом исследователей, включая и автора, в данном пособии не рассматриваются, поскольку оно должно служить целям безопасности и не превращаться в наставление по реализации преступных замыслов.

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, съемный жесткий магнитный диск емкостью не менее 100 Гбайт с интерфейсом IDE или Serial ATA, и устройством Mobile Rack.

Требования по обеспечению информационной безопасности: при проведении лабораторных работ: все компьютеры на время проведения лабораторных работ 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.

Перед изучением дисциплины рекомендуется повторно изложить обучаемым комментарий к ст. 273 УК РФ и предложить им расписаться в журнале инструктажа или в отдельном листе под формулировкой «Об уголовной ответственности за создание и распространение вредоносных программ для ЭВМ предупрежден».

Доцент кафедры АиДМ

В.В. Бакланов