Лабораторная работа № 5

Защита ПК от вредоносных закладок (разрушающих программных средств)

Цель работы:

Закрепление теоретического материала по изучению действия и защите от вредоносных закладок (разрушающих программных средств).

Изучение способов и правил защиты системы от вредоносных закладок (разрушающих программных средств).

Приборы и оборудование:

Персональный компьютер

ОС MS Windows 7 (MS Windows 10), MS Office, Браузер Microsoft Internet Explorer (Edge)

Пояснения к работе и задание:

К основным разновидностям вредоносного воздействия относятся воздействие на информацию (уничтожение, искажение, модификация) и воздействие на систему (вывод из строя, ложное инициирование действия, модификация содержания выполняемых функций, создание помех в работе). Более детально возможный характер воздействия закладок будет представлен ниже при рассмотрении вопроса об их классификации.

Данный вид защиты для ПК имеет особое значение по ряду причин, а именно:

1) он актуален для всех без исключения пользователей ПК независимо от того, конфиденциальная или открытая информация ими обрабатывается;

2) заражение разрушающими программными средствами (РПС) представляет угрозу повышенной опасности для ПК, чему особенно способствует высокий динамизм обмена информацией как по каналам связи (в сетях ЭВМ), так и посредством гибких дисков;

3) защита ПК от РПС требует особого профессионализма, поскольку многие из них носят специфический индивидуальный характер, а их нейтрализация и устранение сопряжены с программными манипуляциями нередко весьм'а сложного и даже искусного характера.

Известные в настоящее время закладки осуществляются аппаратным или программным путем.

Аппаратные закладки могут быть осуществлены в процессе изготовления ПК, ее ремонта или проведения профилактических работ. Реальная угроза таких закладок создается массовым и практически неконтролируемым распространением ПК. Особая опасность аппаратных закладок заключается в том, что они могут длительное время не проявлять своих вредоносных воздействий, а затем начать их осуществление или по истечении определенного времени, или при наступлении некоторого состояния ПК (например, при заполнении данными жесткого магнитного диска до заданного уровня), или по специальной, подаваемой дистанционно команде. Заблаговременное обнаружение аппаратных закладок возможно только в условиях проверок с использованием специальных методов и средств.

Программные закладки (РПС) с точки зрения массового пользователя представляются особо опасными в силу сравнительной (относительно аппаратных) простоты их осуществления, высокой динамичности их распространения и повышенной трудности защиты от них. Так, если в итоге специальных проверок аппаратные закладки не были обнаружены или они были ликвидированы

(нейтрализована возможность их действия), то с высокой степенью можно быть уверенными в их отсутствии в соответствующей ПК. Программные же закладки могут появиться в любое время, чему особенно способствуют следующие обстоятельства:

1) массовый обмен информацией на гибких МД, принявший к настоящему времени характер броуновского движения;

2) широкое распространение копий программ, приобретенных незаконным путем;

3) возможности дистанционного воздействия на ПК, подключенные к сети;

4) широкий и непрерывно растущий диапазон разновидностей закладок, что усложняет процессы их обнаружения и нейтрализации.

В силу изложенных причин защиту от программных закладок рассмотрим несколько детальней, выделив при этом следующие вопросы:

1. Классификация закладок и их характеристики.

2. Принципиальные подходы и общая схема защиты от закладок.

3. Методы и средства защиты.

2. Рекомендации пользователям ПК по защите от программных закладок.

Классификация закладок и их общие характеристики

К сожалению, научно обоснованная классификация закладок до настоящего времени пока не разработана, что объясняется отчасти недостаточным объемом статистических данных, а отчасти тем, что работы по защите от закладок различных разновидностей ведутся изолированно. Системные исследования и разработки еще только предстоит выполнить. Поэтому излагаемое ниже должно рассматриваться лишь в качестве первого приближения.

Всякая классификация осуществляется по вполне определенному и существенно значимому критерию или по их совокупности. Исходя из целей защиты от вредоносного воздействия закладок, их целесообразно классифицировать по следующей совокупности критериев:

1) характеру вредоносного воздействия на АСОД;

2) способу реализации;

3) способу проникновения в АСОД;

4) способность к саморазмножению.

Основные значения *первого* критерия могут быть представлены в следующем виде:

1) уничтожение или искажение программ и/или массивов данных;

2) формирование каналов несанкционированного получения информации;

3) вывод АСОД из числа действующих, т. е. приведение ее в такое состояние, при котором она не может осуществлять свои основные функции;

4) инициирование выполнения предусмотренных в АСОД функций (например, ложная подача команды на остановку производства в автоматизированных системах управления технологическими процессами);

5) создание препятствий в выполнении функций АСОД (например, блокировка отображения информации на экране дисплея, выдачи на печать и др.).ъ

Возможные значения *второго* критерия (способ реализации) могут быть представлены следующим перечнем:

1) аппаратный;

2) программный;

3) организационный.

Первые два способа реализации рассмотрены выше, они, вообще говоря, являются основными. Однако в общем случае можно предположить возможность создания также организационных закладок. Например, в инструкции об уничтожении информации, находящейся в ЭВМ, в злоумышленных целях можно предусмотреть преждевременное ее уничтожение или, наоборот, сохранение той информации, которую надлежало бы уничтожить. В инструкции по использованию криптографических средств злоумышленно можно внести такие положения, выполнение которых может дать крипто-аналитику дополнительную информацию, облегчающую криптоанализ шифртекста. Нетрудно предположить возможность создания ряда других организационных закладок.

По способу проникновения в АСОД *(третий* критерий классификации) закладки могут быть разделены на следующие группы:

1) злоумышленно создаваемые в процессе производства аппаратуры ЭВТ и компонентов ее программного обеспечения;

2) бессознательно вносимые персоналом или пользователями АСОД в процессе ее функционирования;

3) злоумышленно вносимые в процессе функционирования АСОД;

4) злоумышленно создаваемые в процессе ремонта аппаратуры или модификации АСОД.

Наконец, по способности к размножению *(четвертый* критерий классификации) закладки естественным образом делятся на две разновидности:

1) саморазмножаюшиеся;

2) несаморазмножаюшиеся.

К настоящему времени известно значительное количество закладок, получивших такие условные наименования: троянский конь, бомба, ловушка, люк, вирус, червь.

Отличительные особенности данных разновидностей могут быть охарактеризованы следующим образом.

Троянский конь — несаморазмножающееся РПС, способное осуществлять несанкционированное считывание данных, их уничтожение и другие деструктивные функции.

Бомба — несаморазмножающееся РПС одноразового использования, приводящееся в действие в определенных условиях (в задан-

ное время, в заданном состоянии ЭВМ, по команде извне) и осуще-ствляющее крупномасштабное уничтожение информации.

Ловушка — несаморазмножающаяся программа, осуществляющая несанкционированный перехват информации и запись ее в соответствующее поле ЗУ или выдачу в канал связи.

Люк — несаморазмножающаяся программа, обеспечивающая злоумышленнику возможности несанкционированного доступа к защищаемой информации.

Вирус — саморазмножающееся РПС, способное уничтожать или изменять данные и/или программы, находящиеся в ЭВМ.

Червь — саморазмножающееся РПС, способное уничтожать элементы данных или программ.

Принципиальные подходы и общая схема защиты от закладок. Основу защиты составляют следующие функции:

1) создание таких условий, при которых дестабилизирующие факторы (ДФ) не могут появляться;

2) предупреждение появления ДФ, даже если для этого имеются условия; _

3) обнаружение появления ДФ;

4) предупреждение воздействия на информацию появившихся

ДФ;

5) обнаружение негативного воздействия ДФ на информацию;

6) локализация негативного воздействия ДФ на информацию;

7) ликвидация последствий воздействия ДФ.

Методы и средства защиты. Для защиты от закладок должны использоваться методы анализа, синтеза и управления, организационно-правовые, аппаратные и программные средства. Ниже приво^ дятся общие сведения о средствах, специфических для защиты от закладок.

Средства борьбы с вирусами и другими вредоносными закладками можно разделить на юридические, организационно-административные, аппаратные и программные.

Юридические средства сводятся к установлению ответственности за умышленное создание и распространение вирусов и других закладок в целях нанесения ущерба, хотя доказать авторство и умышленность создания таких программ довольно трудно.

Следует признать, что на Западе соответствующие правовые нормы разработаны гораздо лучше, чем в России. Назовем некоторые законы, применяемые в западных странах для борьбы с компьютерными преступлениями:

1) Закон о поддельных средствах доступа, компьютерном мошенничестве и злоупотреблении (США).

2) Федеральный закон о частной тайне (США).

3) Закон о предупреждении экономических преступлений (Германия).

4) Закон об авторском праве (Германия).

5) Федеральный закон о защите данных (Германия).

6) Закон об авторском праве и поправки к нему (Великобритания).

7) Закон о защите данных (Великобритания).

8) Закон об обработке данных, о файлах данных и личных свободах (Франция).

В ряде стран введены соответствующие статьи в уголовные кодексы.

Перечисленные законы позволяют вести достаточно эффективную борьбу с изготовителями вредоносных программ. Например, еще в начале 1989 года американский студент был приговорен судом к трем месяцам тюремного заключения и штрафу в 270 тысяч долларов за разработку вируса, которым были выведены из строя шесть тысяч компьютеров Министерства обороны США.

В Российской Федерации в последнее время также предпринимаются серьезные усилия по созданию юридической основы борьбы с рассматриваемыми угрозами. Так, в принятый недавно Уголовный кодекс Российской Федерации введено три статьи (272—274), по которым предусмотрена ответственность за компьютерные преступления, причем самое строгое наказание (от 3 до 7 лет тюремного заключения) предписывается статьей 273 — за создание, использование и распространение вредоносных программ.

Организационно-административная защита от вредоносных программ заключается в выработке и неукоснительном осуществлении организационных и

организационно-технических мероприятий, направленных на предупреждение заражения компьютеров этими программами, обнаружение заражения, нейтрализацию негативного их воздействия и ликвидацию последствий. Названные мероприятия должны осуществляться как в организациях — разработчиках программных средств, так и в организациях, эксплуатирующих эти программы.

В организациях-разработчиках весьма целесообразно из состава высококвалифицированных программистов создавать специальные группы для выполнения следующих функций:

1) определения потенциально возможных источников вредоносных программ и выработка рекомендаций по их обходу;

2) выявления и изучения всех нештатных ситуаций, возникающих при разработке программного обеспечения, документального

оформления результатов анализа и оповещение всех заинтересованных при выявлении опасностей;

3) регулярного контроля состояния программного обеспечения и средств борьбы с вредоносными программами;

4) возможно более быстрой ликвидации последствий произошедшей атаки вредоносных программ и изготовления соответствующих средств защиты;

5) оказания методической помощи своим абонентам в организации необходимой защиты от вредоносных программ.

Основными мероприятиями по защите программ и данных в организациях, использующих программы, представляются следующие:

1) приобретение только законным путем необходимых технических средств и программ, сертифицированных на отсутствие вредоносных закладок;

2) создание эталонных копий основных программ и резервирование баз данных;

3) организация автоматизированной обработки данных с соблюдением всех приемов и правил;

4) периодическая тщательная проверка состояния программного обеспечения и баз данных;

5) проверка психологических особенностей сотрудников при приеме на работу;

6) создание и поддержание в коллективах здорового морально-психологического климата.

Из аппаратных средств защиты рекомендуются следующие:

1) форматирование диска (для винчестера — полное стирание и переразметка), перезагрузка операционной системы и восстановление программ с незараженных копий;

2) заклеивание (закрывание) отверстия защиты записи дискеты;

3) физическая блокировка ключом клавиатуры ЭВМ;

4) запрет и регистрация попыток записи в файлы операционной системы в области памяти, занятые системной информацией.

Известны и другие, подобные перечисленным, меры: разделение областей памяти между программами, разделение программ по приоритетам и т. п.

В целях повышения эффективности защиты ЭВМ от вредоносных программ в последнее время ведутся разработки защищенных противовирусных компьютеров и специальных плат, встраиваемых в существующие компьютеры.

Важнейшим компонентом среди средств защиты от вредоносных программ выступают специальные программы, получившие на звание антивирусных. Известные к настоящему времени антивирусные программы по функциональному признаку делятся на 4 класса:

— класс А — предупреждение заражения;

— класс Б — выявление последствий заражения;

— класс В — минимизация причиненного ущерба;

— класс Г — общего характера.

Программы класса А делятся на 5 групп следующего назначения:

А1 — фильтры, следящие за операциями других исполняемых программ и реагирующие на подозрительные действия;

А2 — резидентные детекторы и фаги, следящие за появлением в оперативной памяти конкретных вирусов и подающие при их появлении специальные сигналы оператору;

А3 — иммунизаторы, изменяющие файлы и области оперативной памяти таким образом, что вирус их после этого не заражает;

А4 — разграничители доступа, ограничивающие распространение вирусов путем разграничения доступа к ресурсам ЭВМ, программам и массивам данных со стороны других программ и пользователей;

А5 — преобразователи параметров операционной среды, реализующие изменение соглашений, принятых в операционной системе (форматы записей, команды, расположение системной информации и др.), недоступные разработчикам вирусов и тем самым препятствующие заражению ЭВМ.

Программы класса Б делятся на 6 групп следующего функционального назначения:

Б1 — нерезидентные детекторы и фаги, осуществляющие просмотр запоминающих устройств, определяющие зараженность файлов и дисков и организующие их лечение;

Б2 — программы проверки подозрительных характеристик, осуществляющие просмотр запоминающих устройств и выявление таких характеристик, которые могут говорить о наличии вируса в системе. К таким характеристикам относятся недопустимые значения отдельных полей в заголовке файла, подозрительные переходы, странные изменения в программах и т. п.;

Б3 — программы, осуществляющие просмотр файлов и носителей, определение различных их характеристик (контрольные суммы, криптографические суммы, длины, даты и времени создания и др.) и сравнение этих величин с эталонами в целях определения возможного заражения;

Б4 — программы, осуществляющие слежение и регистрацию в системном журнале операций, осуществляемых на ЭВМ. При зара-

жении анализ журнала помогает выявить источник заражения, характер поведения вируса;

Б5 — программы-ловушки (дрозофилы, уловители), специально выделяемые для заражения, которые, заражаясь, сигнализируют о наличии вируса;

Б6 — программы автономной защиты файла, защищающие файлы от вирусов путем дописывания своей копии к защищаемым модулям.

Программы класса В (минимизирующие ущерб, причиненный заражением РПС) делятся на следующие 3 группы:

В1 — программы полного копирования, предназначенные для создания резервных копий программного обеспечения;

В2 — программы частичного копирования, предназначенные для копирования и восстановления наиболее уязвимых частей диска (Boot-сектор, FAT, корневое оглавление);

В3 — программы, прерывающие вычислительный процесс, т. е. осуществляющие принудительное прерывание вычислительного процесса в целях локализации распространения вируса.

Программы класса Г (общего назначения) предназначены не для прямой борьбы с вирусами, а для оказания помощи в этой борьбе. Эти программы делятся на 5 групп следующего назначения:

Г1 — программы просмотра диска, позволяющие отображать значения каждого сектора, копировать одну физическую область в другую. Применяются для определения целостности отдельных частей диска, наличия вируса в файлах и внесения небольших изменений;

Г2 — программы, позволяющие искать на диске контекст определенного содержания. С их помощью можно найти участки кодов вирусов и пораженные ими сектора;

ГЗ — программы, позволяющие восстанавливать отдельные части диска;

Г4 —. программы, реализующие просмотр состояния оперативной памяти, состав и характеристики находящихся там модулей;

Г5 — программы, позволяющие упорядочить информацию на диске на физическом уровне по заранее заданному закону.

Контрольные вопросы:

1. Перечислите уровни защиты компьютерных и информационных ресурсов.
2. Дайте понятие вредоносных закладок (разрушающих программных средств), перечислите разновидности и особенности.

Какие действия в рамках защитных мероприятий требуется выполнять для защиты от РПС?