Системы защиты программного обеспечения

Подготовили: Баум А.,

Залгараев Р. Калиновский А.,

Кариков А., Каримов Р.,

Садырбаев Д.

Программное обеспечение (ПО) – совокупность специальных программ, облегчающих процесс подготовки задач к выполнению на ЭВМ и организующих прохождение их через машину, а также процедур, описаний, инструкций и правил вместе со всей связанной с этими компонентами документацией, используемых при эксплуатации вычислительной системы.

В настоящее время одним из наиболее опасных средств информационного воздействия на компьютерные системы являются программы - вирусы или компьютерные вирусы.

В качестве основных средств вредоносного (деструктивного) воздействия на КС рассматривают алгоритмические и программные закладки. Под алгоритмической закладкой понимается преднамеренное скрытое искажение части алгоритма программы, в результате чего возможно появление у программного компонента функций, не предусмотренных спецификацией и выполняющихся при определенных условиях протекания вычислительного процесса. Программная закладка - это внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций, позволяющих осуществлять несанкционированные воздействия на информацию.

Выделяют различные методы анализа безопасности программного обеспечения:

**Контрольно-испытательные методы** - это методы, в которых критерием безопасности программы служит факт регистрации в ходе тестирования программы нарушения требований по безопасности, предъявляемых в системе предполагаемого применения исследуемой программы. Тестирование может проводиться с помощью тестовых запусков, исполнения в виртуальной программной среде, с помощью символического выполнения программы, ее интерпретации и другими методами.

**Логико-аналитические методы.** При проведении анализа безопасности с помощью логико-аналитических методов строится модель программы и формально доказывается эквивалентность модели исследуемой программы и модели РПС. В простейшем случае в качестве модели программы может выступать ее битовый образ, в качестве моделей вирусов множество их сигнатур, а доказательство эквивалентности состоит в поиске сигнатур вирусов в программе. Более сложные методы используют формальные модели, основанные на совокупности признаков, свойственных той или иной группе РПС.

Программно-технические средства защиты ПО

-Парольная защита;

-Системы «привязки» ПО;

-Средства защиты ПО с электронными ключами;

-Средства защиты ПО с ключевыми дисками.

**Парольная защита**

**Положительные** стороны парольной защиты: надёжная защита от злоумышленника-непрофессионала; минимальные неудобства для пользователя; возможность передачи пароля/кода по сети; отсутствие конфликтов с системным и прикладным ПО и аппаратным обеспечением; **Отрицательные** стороны парольной защиты: низкая стойкость большинства систем защиты данного типа; пользователю необходимо запоминать пароль/код.

**Системы «привязки»** **ПО**

**Положительные** факторы: не требуется добавочных аппаратных средств для работы защиты; затруднение несанкционированного доступа к скопированному ПО; простота применения.

**Отрицательные** факторы: ложные срабатывания СЗПО при любых изменениях в параметрах ПК; низкая стойкость при доступе злоумышленника к ПК пользователя; возможность конфликтов с системным ПО.

**Средства защиты ПО с электронными ключами**

**Положительные** факторы: значительное затруднение нелегального использования ПО; избавление производителя ПО от разработки собственной системы защиты; высокая автоматизация процесса защиты ПО; наличие API системы для более глубокой защиты; возможность легкого создания демо-версий; достаточно большой выбор таких систем на рынке.

**Отрицательные** факторы: затруднение разработки и отладки ПО из-за ограничений со стороны средств защиты; дополнительные затраты на приобретение системы защиты и обучение персонала; замедление продаж из-за необходимости физической передачи аппаратной части; повышение системных требований из-за защиты; снижение отказоустойчивости ПО; несовместимость систем защиты и системного или прикладного ПО пользователя; несовместимость защиты и аппаратуры пользователя; несовместимости электронных ключей различных фирм; снижение расширяемости компьютерной системы; наличие у аппаратной части размеров и веса; угроза кражи аппаратного ключа.

**Правовые средства защиты ПО**

-Лицензирование ПО

-Патентование ПО

-Авторское право

-Метод авторизации ПО через Интернет

ILOVEYOU (ЯТЕБЯЛЮБЛЮ), также известный как LoveLetter (ЛюбовноеПисьмо) — компьютерный вирус, который успешно атаковал миллионы компьютеров под управлением Windows в 2000 году. Вирус был разослан на почтовые ящики с Филиппин в ночь с 4 мая на 5 мая 2000 года; в теме письма содержалась строка «ILoveYou», а к письму был приложен скрипт «LOVE-LETTER-FOR-YOU.TXT.vbs». В большинстве случаев пользователь открывал вложение. При открытии вирус рассылал копию самого себя всем контактам в адресной книге Microsoft Outlook. Он также перезаписывал файлы определённых типов и распространялся через IRC-каналы, создавая файл LOVE-LETTER-FOR-YOU.HTM в системном каталоге Windows. В общей сложности, вирус поразил более 3 миллионов компьютеров по всему миру. Предполагаемый ущерб, который червь нанёс мировой экономике, оценивается в размере до 10 миллиардов долларов, за что вошёл в Книгу рекордов Гиннесса как самый разрушительный компьютерный вирус в мире.

На уровне машинной системы ILOVEYOU полагался на включенную системную настройку механизма сценариев[1] (который запускает файлы на языке сценариев, такие как файлы .vbs) и воспользовался функцией Windows, которая по умолчанию скрывает расширения файлов, что авторы вредоносных программ использовали в качестве эксплойта. Windows разбирает имена файлов справа налево, останавливаясь на первом символе точки и показывая только те элементы, которые находятся слева от него.