Основные понятия в области защиты ПО

Защита ПО – это комплекс мер, направленных на защиту программного обеспечения от несанкционированного приобретения, использования, распространения, модифицирования, изучения и воссоздания аналогов.

Причины использования систем защиты ПО:

1. незаконное использование алгоритмов, являющихся интеллектуальной собственностью автора, при написании аналогов продукта (промышленный шпионаж);
2. несанкционированное использование ПО (кража и копирование);
3. несанкционированная модификация ПО с целью внедрения программных злоупотреблений;
4. незаконное распространение и сбыт ПО (пиратство).

ПО должно быть защищено от воздействия:

- ✔ человека.;
- ✔ аппаратуры;
- ✔ специализированных программ

Системы защиты ПО по методу установки можно подразделить на

- ✔ системы, устанавливаемые на скомпилированные модули ПО;
- ✔ системы, встраиваемые в исходный код ПО до компиляции;
- ✔ комбинированные

По используемым механизмам защиты средства защиты делятся на:

1. системы, использующие сложные логические механизмы - различные методы и приёмы, ориентированные на затруднение дизассемблирования, отладки и анализа алгоритма СЗ и защищаемого ПО;

Дизассемблирование – процесс и/или способ получения исходного текста программы.

По используемым механизмам защиты средства защиты делятся на:

2. системы, использующие шифрование защищаемого ПО – для дезактивации защиты необходимо определение ключа дешифрации ПО;
3. комбинированные системы.

Методы, препятствующие дизассемблированию информации

- шифрование;
- архивация:
- использование самогенерирующих кодов;
- «обман» дизассемблера.

Обзор методов защиты программного обеспечения

1. Организационные меры

Полноценное использование программного продукта невозможно без соответствующей поддержки со стороны производителя: подробной пользовательской документации, «горячей линии», системы обучения пользователей и т.п.

2. Правовые меры

Заключаются в установлении ответственности за использование программного обеспечения с нарушением порядка, установленного действующим законодательством.

3. Технические средства

Можно классифицировать по способу распространения защищаемого программного обеспечения и типу носителя лицензии.

Локальная программная защита

Подразумевает необходимость ввода серийного номера (ключа) при установке или запуске программы.

В настоящий момент метод используется только в совокупности одним или более других методов.

Сетевая программная защита

Осуществляемое программой сканирование сети исключает одновременный запуск двух программ с одним регистрационным ключом на двух компьютерах в пределах одной локальной сети.

Глобальная программная защита

Если программа работает с каким-то централизованным сервером и без него бесполезна, она может передавать серверу свой серийный номер; если номер неправильный, сервер отказывает в услуге.

Недостаток: существует возможность создать сервер, который не делает такой проверки.

Защита при помощи компакт-дисков

Программа требует оригинальный компакт-диск.

Для защиты от копирования используется:

- ✔ запись информации в неиспользуемых секторах;
- ✔ проверка расположения и содержимого «сбойных» секторов;
- ✔ проверка скорости чтения отдельных секторов.

Программно-аппаратные средства защиты ПО с электронными ключами

Электронный ключ – это аппаратная часть системы защиты, представляющая собой плату с микросхемами памяти либо с микропроцессором, помещенную в корпус и предназначенную для установки в один из стандартных портов ПК или слот расширения материнской платы.

Электронный ключ содержит ключевые данные, называемые также лицензией, записанные в него разработчиком защищенной программы.

Защита программы основывается на том, что только ему (разработчику) известен полный алгоритм работы ключа.

Виды электронных ключей

- ✔ ключи с памятью (без микропроцессора);
- ✔ ключи с микропроцессором (и памятью).

Ключи с памятью хранят критическую информацию (ключ дешифрации, таблица переходов) в памяти электронного ключа.

Для дезактивации необходимо наличие у злоумышленника аппаратной части системы защиты, либо снятие логической защиты.

Ключи с микропроцессором содержат в аппаратной части не только ключ дешифрации, но и блоки шифрации/дешифрации данных, при работе защиты в электронный ключ передаются блоки зашифрованной информации, и принимаются расшифрованные данные

Достоинства:

1. Ключ можно использовать в любом компьютере, на котором необходимо запустить программу.
2. Значительное затруднение нелегального распространения и использования ПО.
3. Избавление производителя ПО от разработки собственной системы защиты.
4. Высокая автоматизация процесса защиты ПО.

Недостатки:

1. Дополнительные затраты на приобретение системы защиты и обучение персонала.
2. Замедление продаж из-за необходимости физической передачи аппаратной части.
3. Повышение системных требований из-за защиты (совместимость, драйверы).
4. Несовместимость защиты и аппаратуры пользователя.
5. Затруднения использования защищенного ПО в мобильных ПК.

Привязка к параметрам компьютера и активация

В процессе установки программа подсчитывает код активации – контрольное значение, однозначно соответствующее установленным комплектующим компьютера и параметрам установленной программы.

Это значение передается разработчику программы. На его основе разработчик генерирует ключ активации, подходящий для активации приложения только на указанной машине.

Достоинства:

не требуется никакого специфического аппаратного обеспечения

Недостатки:

1. Программное обеспечение становится неработоспособным в случае, если пользователь производит модернизацию компьютера (если привязка осуществляется к аппаратной конфигурации компьютера).
2. Ложные срабатывания СЗПО при любых изменениях в параметрах ПК.
3. Низкая стойкость при доступе злоумышленника к ПК пользователя.
4. Возможность конфликтов с системным ПО.

Алгоритмы защиты ПО

1. **Алгоритмы запутывания** – используются хаотические переходы в разные части кода, внедрение ложных процедур - "пустышек", холостые циклы, искажение количества реальных параметров процедур ПО, разброс участков кода по разным областям ОЗУ и т.п. (метод «спагетти»)

Алгоритмы защиты ПО

2. **Алгоритмы мутации** - создаются таблицы соответствия операндов - синонимов и замена их друг на друга при каждом запуске программы по определенной схеме или случайным образом, случайные изменения структуры программы.

Алгоритмы защиты ПО

3. **Алгоритмы компрессии данных** - программа упаковывается, а затем распаковывается по мере выполнения. (EXEPACK - это один из первых EXE-упаковщиков, разработанный ещё в начале 80-х годов, zLib)

Алгоритмы защиты ПО

4. **Алгоритмы шифрования данных** - программа шифруется, а затем расшифровывается по мере выполнения. (Полная – частичная расшифровка)

Алгоритмы защиты ПО

5. **Методы затруднения дизассемблирования** - используются различные приемы, направленные на предотвращение дизассемблирования в пакетном режиме.

Алгоритмы защиты ПО

6. **Методы затруднения отладки** - используются различные приемы, направленные на усложнение отладки программы.

Алгоритмы защиты ПО

7. Эмуляция процессоров и операционных систем - создается виртуальный процессор и/или операционная система и программа-переводчик из системы команд ПК в систему команд созданного процессора или ОС, после такого перевода ПО может выполняться только при помощи эмулятора, что резко затрудняет исследование алгоритма ПО.

Алгоритмы защиты ПО

8. **Нестандартные методы работы с аппаратным обеспечением** - модули системы защиты обращаются к аппаратуре, минуя процедуры операционной системы, и используют малоизвестные или недокументированные её возможности.

По принципу функционирования СЗ можно подразделить на

- ✔ упаковщики / шифраторы;
- ✔ СЗ от несанкционированного копирования;
- ✔ СЗ от несанкционированного доступа (НСД).

Упаковщики/шифраторы

Используются алгоритмы компрессии данных; приёмы, связанные с использованием недокументированных особенностей операционных систем (ОС), криптографические методы, алгоритмы мутации, запутывание логики программы.

Недостатки:

1. Замедляют выполнение кода ПО.
2. Шифрование / упаковка кода ПО вызывает затруднения при обновлении (update) и исправлении ошибок (bugfix, servicepack).
3. Данный класс систем уязвим, так как программный код, в конечном итоге, распаковывается или расшифровывается для выполнения.
4. Упаковка и шифрование исполняемого кода вступает в конфликт с запрещением самомодифицирующегося кода в современных ОС.

Средства защиты от несанкционированного копирования

Средства защиты от несанкционированного копирования осуществляют "привязку" ПО к дистрибутивному носителю

Достоинства:

1. Затруднение нелегального копирования и распространения ПО;
2. Защита прав пользователя на приобретённое ПО.

Недостатки:

1. Большая трудоёмкость реализации системы защиты;
2. Затруднение продаж из-за необходимости физической передачи дистрибутивного носителя;
3. Снижение отказоустойчивости ПО;
4. На время работы ПО занимается накопитель;

Средства защиты от НСД

Средства защиты от НСД осуществляют предварительную или периодическую аутентификацию пользователя ПО или его компьютерной системы путём запроса дополнительной информации.