АНАЛИЗ СРЕДСТВ ПРЕОДОЛЕНИЯ СИСТЕМ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Сергей Середа,
аспирант Экономической Академии Республики Молдова,
кафедра кибернетики и экономической информатики

В работе рассмотрены вопросы анализа и классификации средств преодоления систем программной защиты ПО. Приведены функциональные возможности и способ применения конкретных видов программных средств. Описаны угрозы системам защиты ПО. По результатам проведенного анализа предметной области сделаны общие выводы о характере применения систем защиты ПО.

Проблемы защиты авторских прав на программное обеспечение в области контроля над его использованием и дальнейшим распространением в настоящее время принято решать при помощи программно-технических средств - систем защиты ПО. Анализ и классификация подобных средств приводятся в [1, 2, 4 и др.]. В то же время для обхода и отключения подобных систем защиты существует множество инструментальных средств. Возникает задача сопоставить возможности средств защиты ПО (СЗПО) с возможностями средств их преодоления. Результаты такого анализа будут полезны для оценки рисков при производстве программных продуктов, а так же планировании и оценке уровня стойкости систем защиты ПО.

В рамках исследования проблем защиты программного обеспечения можно рассматривать три следующих глобальных вопроса:

1. Что защищать?

Вопрос связан с классификацией ПО и оценкой возможностей по защите ПО

2. Как защищать?

Вопрос связан с анализом и классификацией мер и средств защиты ПО

3. От чего защищать?

Вопрос связан с анализом и классификацией угроз ПО и средств их реализации

Если первые два вопроса в настоящее время освещены хотя бы частично, третий вопрос представляет собой серьезное "белое пятно" в области исследований в сфере защиты ПО, хотя определенные исследования по этой теме велись [4, 9]. С другой стороны, без четкого понимания угроз безопасности ПО и возможностей средств реализации подобных угроз сложно вообще говорить об эффективной защите программного обеспечения, что подтверждается существующей практикой в области защиты информационных систем. Следовательно, для серьезного исследования вопросов защиты ПО необходимо осуществить анализ и классификацию средств реализации атак на программное обеспечение.

Данная работа является попыткой осветить вышеописанные вопросы и рассматривает технические (программные) средства преодоления СЗПО.

Следует сразу отметить, что лишь малая часть из рассматриваемых типов программного обеспечения является специфическими программными средствами, предназначенными для несанкционированного отключения систем защиты ПО. Большинство же указанных средств относится к системному программному обеспечению и рассматривается как "инструментарий злоумышленника" в силу двойственности технологий.

В настоящее время существуют лишь неформальные классификации средств преодоления СЗПО, они основываются на традиционно сложившемся разделении программных средств в предметной области и в силу этого являются не совсем полными и частично противоречивыми.

В данной работе предлагается классификация по функциональному признаку (она частично совпадает с "традиционной" классификацией средств преодоления СЗПО), в ее рамках средства упорядочены по степени сложности и стадии анализа исследуемого ПО.

1. Программы-каталогизаторы, или файловые оболочки ОС

В стандартные возможности таких программ входят функции просмотра атрибутов файлов (тип, дата создания/модификации, размер, флаги доступа и др.), подсчета их количества и общего объема в каталоге приложения, просмотра файлов и т.п. При помощи этого типа программных средств, как правило, реализуется ***предварительный анализ защищенных продуктов и первичная локализация СЗПО***.

Примером подобного использования может быть сравнение дат создания всех файлов в каталоге установленного приложения (или системном каталоге). В случае использования системой защиты каких-либо динамических библиотек разница в датах их создания позволит легко локализовать файлы, относящиеся к СЗПО (как правило, даты создания "рабочих" файлов пакета совпадают, дата создания модулей СЗПО отличается

от них, так как СЗПО часто поставляются отдельно как внешняя библиотека).

Аналогичным же образом локализуются и файлы, хранящие счетчики количества запусков ПО, даты этих файлов постоянно обновляются. А при помощи обычного текстового просмотра объектного модуля можно довольно легко определить тип и производителя СЗПО, так как обычно эта информация включается в тело защищенного модуля самой СЗПО.

2. Программы поиска файлов и текстовых и двоичных последовательностей в текстовых и двоичных файлах.

Данный тип программ позволяет производить поиск заданной последовательности (маски поиска) в одном или сразу нескольких файлах с выдачей результатов в виде списка смещений относительно начала файла, по которым был найден искомый фрагмент; а также всех файлов, удовлетворяющих определенному критерию или содержащих вышеописанную последовательность. При помощи указанных средств реализуется ***вторичный анализ СЗПО и локализация ключевых фрагментов СЗПО.***

Обычно средства файлового поиска используются для следующих целей: поиска известных сигнатур СЗПО в объектных модулях; поиска строк с сообщениями СЗПО (например, "Программа не зарегистрирована!" или "Спасибо за регистрацию!"), поиска файлов СЗПО с известными именами/сигнатурами.

Первый и последний виды использования рассматриваемого типа ПО ориентированы на отыскание стандартных элементов СЗПО, исследованных ранее и адаптации "типовых решений" к исследуемой версии СЗПО. Второй вид использования поисковых программ ориентирован на локализацию процедур СЗПО, отвечающих за идентификацию и аутентификацию легального пользователя ПО. Большинство СЗПО реализует в процессе своей работы диалог с пользователем (как минимум на уровне сообщений об ошибках), локализация элементов этого диалога позволяет довольно легко локализовать "ядро" СЗПО, а иногда даже определить пароль легального пользователя.

3. Программы - мониторы файловой системы (File Monitors)

Этот тип ПО позволяет отслеживать изменения, происходящие в файловой системе при запуске определенных программ. В большинстве таких программ предусмотрена система фильтров для формирования протоколов работы отдельных приложений. При помощи данного типа средств ***реализуется анализ работы СЗПО с файлами.***

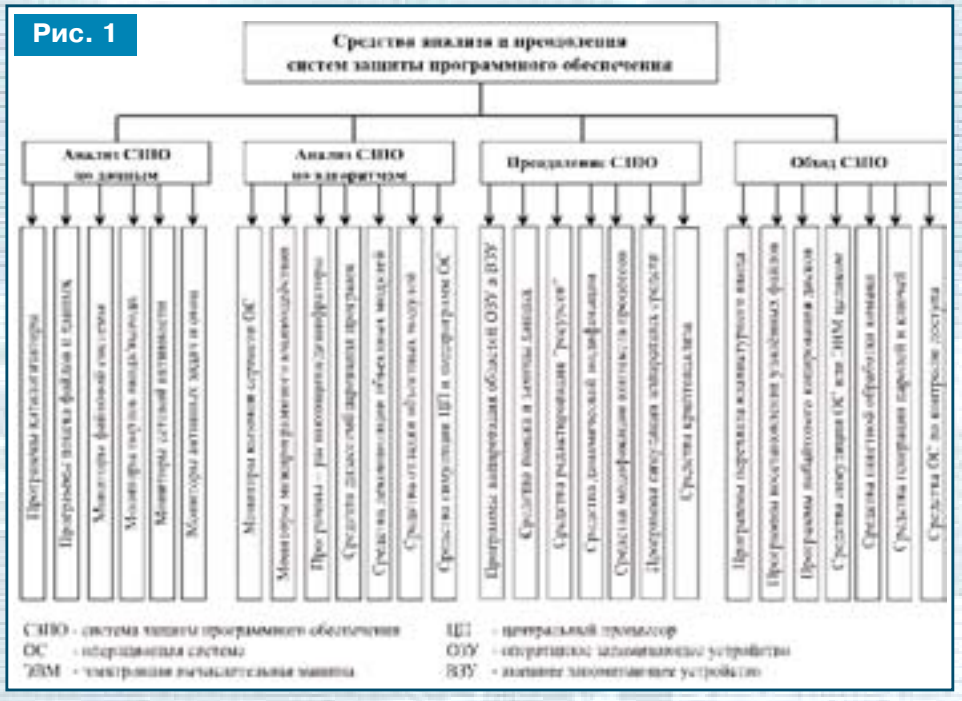
Например, подобные программы позволяют выяснить, что именно и где изменяют распознанные на этапах первичного и вторичного анализа модули СЗПО, либо определить модуль, производящий изменения в определенном файле. Эта информация позволяет точно локализовать счетчики количества запусков ПО, скрытые файлы систем "привязки" ПО, "ключевые файлы", файлы с информацией о функциях ПО, разрешенных для использования в рамках данной лицензии на продукт и т.п., а также модули и конкретные процедуры СЗПО, работающие с этими данными.

4. Программы - мониторы системных файлов ОС (Registry Monitors)

Программные средства этого типа предназначены для отслеживания изменений, вносимых приложениями в конфигурационные файлы ОС. В рассматриваемом контексте данные программы позволяют ***реализовать анализ работы СЗПО с системными файлами*** (более специфично для ОС семейства Windows).

Рассматриваемые средства позволяют определять, работает ли СЗПО с файлами конфигурации ОС, какие изменения она туда вносит и какие данные использует. В результате подобного анализа становится возможным обнаружить скрытые счетчики количества запусков ПО, сохраненные даты первой установки ПО на ЭВМ пользователя, записи с лицензионными ограничениями функциональности ПО и т.п. Такой анализ дает результаты, подобные результатам анализа работы СЗПО с файлами.

Рис. 1



5. Программы - мониторы вызовов подпрограмм ОС (API Monitors)

ПО этого типа предназначено для отслеживания вызова системных функций одним или несколькими приложениями с возможностью фильтрации/выделения групп отслеживаемых системных функций или приложений. Применение таких программ позволяет проводить ***анализ использования СЗПО системных функций.***

Учитывая, что все действия ПО (и СЗПО), связанные с работой с файловой системой, работой с конфигурацией ОС, реализацией диалога с пользователем, работой с сетью и многим другим, реализуются посредством вы-

зова функций ОС. Анализ использования СЗПО системных функций позволяет довольно подробно изучить механизмы работы систем защиты, найти их слабые места и разработать пути их обхода.

Например, практически все современные системы защиты от копирования оптических дисков базируются на довольно небольшом наборе системных функций по работе с данным видом накопителей информации, отслеживание этих функций позволяет найти и нейтрализовать механизмы проверки типа носителя внутри СЗПО.

6. Программы - мониторы обмена данными с системными устройствами (портами) (Port Monitors)

В современной архитектуре ОС доступ ко всем системным устройствам (их контроллерам) осуществляется через т.н. "порты ввода/вывода". Все современные ОС виртуализируют эти порты, организуя таким образом совместный доступ нескольких приложений к одному и тому же порту (используя механизм очереди), а также осуществляя контроль доступа к портам в целях обеспечения безопасности ОС. Использование этого типа программных средств позволяет проводить ***анализ взаимодействия СЗПО с системными устройствами.*** Контролируя доступ и обмен данными через порты ввода/вывода программной и аппаратной частей СЗПО, можно анализировать и преодолевать механизмы таких типов защит, как СЗПО с электронными ключами, СЗПО с ключевыми дисками и СЗПО "привязки" к ЭВМ пользователя.

7. Программы - мониторы сетевого обмена данными (Network Traffic Monitors)

Рассматриваемый тип программ предназначен для отслеживания сетевой активности приложений в рамках ОС. Как правило, такие программы позволяют фильтровать/выделять приложения или сетевые соединения по вводимым критериям. Использование сетевых мониторов позволяет проводить ***анализ сетевого обмена СЗПО.***

Целый ряд современных программных продуктов реализует проверку аутентичности пользователя путем запроса данных о состоянии лицензии для данной рабочей станции с "сервера лицензий" в ЛВС. Также в последнее время появились программные продукты, проверяющие аутентичность пользователя или срок своего использования через Интернет. Кроме указанных видов ПО, существуют также условно бесплатные программные продукты (ППр), в которых временные или функциональные ограничения заменены обязательным просмотром рекламной информации, получаемой через Интернет. Отслеживая сетевой обмен подобных ППр, можно анализировать механизмы систем их защиты.

8. Программы - мониторы активных задач, процессов, потоков и окон (Process/Windows Managers)

Указанный тип программных средств предназначен для отслеживания и управления объектами ОС (задачами, процессами, потоками, окнами и др.). Подобные программы обычно предоставляют возможности поиска необходимого объекта ОС, переключения на него управления, изменения его приоритета, уничтожения объекта, сохранения его параметров (а иногда и содержимого) на диске.

Применение мониторов задач дает возможность производить ***анализ модульной структуры СЗПО.*** Подобный анализ позволяет выяснить подробности организации СЗПО во время ее работы. Список динамически загружаемых процессом библиотек, данные о количестве создаваемых и уничтожаемых приложением потоков и окон, поведение ППр при попытке принудительно завершить процесс, содержащий СЗПО, позволяют существенно дополнить картину анализа функционирования системы защиты.

9. Программы - мониторы конвейеров данных, системных сообщений и высокоуровневого межпрограммного взаимодействия (Message/COM hooks)

Средства данного типа предназначены для отслеживания сообщений, данных и вызовов подпрограмм, которыми обмениваются объекты ОС. Применение мониторов сообщений позволяет производить ***анализ межмодульного взаимодействия в рамках СЗПО*** (более специфично для ОС семейства Windows).

В результате такого анализа получается информация о протоколах обмена данными между различными частями системы защиты, условиях ее срабатывания и отключения, динамике функционирования защиты.

10. Программы перехвата и протоколирования клавиатурного ввода (Keyboard Loggers)

Данный тип программных средств предназначен для сохранения информации, введенной в ЭВМ с клавиатуры в специальные файлы протокола, возможна фильтрация сохраняемых данных по дополнительно вводимым критериям. "Клавиатурные шпионы" никак не связаны с анализом СЗПО, но предоставляют возможность осуществить **незаконное получение ключа регистрации/пароля к ПО, защищенному парольной СЗПО.**

11. Программы копирования областей ОЗУ в ВЗУ (Memory Dumpers)

Указанный тип программных средств предназначен для сохранения областей оперативной памяти, в том числе памяти выполняемых программ, на диск. В рамках исследования СЗПО данные средства позволяют произвести **принудительное сохранение образа памяти защищенного приложения.**

В случае использования механизмов шифрования/упаковки объектного кода защищаемого ПО, сохранение памяти активного процесса ОС позволяет получить копию (незначительно модифицированного загрузчиком ОС) кода защищаемого ПО в "открытом виде". В результате таких действий возможно либо сразу получить экземпляр незащищенного программного продукта, либо получить важную для дальнейшего анализа СЗПО информацию.

Очень большое число "защищенных" программных продуктов представляет собой упакованные и/или зашифрованные объектные модули без какой-либо серьезной внутренней алгоритмической защиты ПО.

12. Программы восстановления удаленных файлов (Unerase/Undelete Utilities)

Подобные программные средства предназначены для восстановления файлов, которые были (ошибочно) удалены из доступной пользователю области файловой системы ОС и не были еще перезаписаны новыми данными.

Применение программ указанного типа к СЗПО позволяет принудитель-

но восстанавливать временные файлы СЗПО, использованные ими в процессе работы; восстанавливать в полном объеме распакованные и частично удаленные дистрибутивы ПО и временные файлы ОС. Так реализуется ***повторное использование объектов СЗПО.*** Например, ряд СЗПО производит распаковку/дешифрацию объектных модулей ПО в специальные временные файлы, которые затем запускаются на выполнение, а после отработки стираются. Восстановление таких файлов позволяет преодолеть защиту ПО.

13. Программы побайтового копирования гибких магнитных дисков (ГМД), оптических дисков (ОД) и жестких магнитных дисков (ЖМД) (Byte Copiers, CD Rippers)

Данный тип программных средств предназначен для создания максимально точных копий физической структуры носителей данных без учета их логической структуры. Обычно подобные программы предоставляют возможность сохранения таких "слепков" в виде файлов на диске. При помощи приведенного типа средств реализуется **преодоление СЗПО от копирования, СЗПО с ключевыми дисками и СЗПО с "привязкой" к компьютерной системе пользователя** (к жесткому диску).

В настоящий момент чрезвычайно популярными являются СЗПО от копирования для компьютерных игр, распространяемых на оптических дисках формата CD и Sony PS. Не меньшей популярностью пользуются и средства побайтового копирования оптических дисков (для создания "пиратских" дисков) и средства сохранения содержимого оптических дисков в виде файлов на жестких дисках (для получения возможности использования ПО, не занимая накопитель).

14. Программы - распаковщики/дешифраторы (Unpackers/Decryptors)

Средства распаковки/дешифрации объектных модулей позволяют получать копии указанных модулей в том виде (или близком к таковому), в каком они были до их упаковки/шифрации. По функциональному содержанию эти программы близки к средствам сохранения областей ОЗУ на диске, но данный тип программных средств, во-первых, отличается высокой специализацией (то есть направленностью на какой-то один тип или класс средств упаковки/шифрации), а во-вторых, не всегда требует загрузки обрабатываемого объектного модуля в ОЗУ как процесса ОС.

При использовании подобных программ реализуется **преодоление СЗПО пакующего или шифрующего типа.** Как правило, распаковка/дешифрация защищенных объектных модулей ПО производится для получения возможности более глубокого дальнейшего анализа СЗПО.

15. Средства дизассемблирования объектных модулей ПО (Disassemblers)

Программы этого типа предназначены для "детрансляции" объектных модулей из машинного кода в мнемокод ассемблера. При применении средств дизассемблирования производится **статический анализ алгоритмов СЗПО по мнемокоду.**

Получение доступа к мнемокоду СЗПО дает превосходную возможность детального анализа программного и алгоритмического исполнения процедур СЗПО, а также нахождения конкретных путей обхода или модификации ключевых фрагментов СЗПО. Иногда появляется возможность использования элементов СЗПО во вновь создаваемых средствах их преодоления.

16. Средства декомпиляции объектных модулей ПО (Decompilers)

Декомпилирующие программы сходны дизассемблерам и даже иногда их используют в качестве своих подпрограмм. Задачей, стоящей перед данным типом программных средств, является "детрансляция" объектных модулей из машинного кода в исходный код на языке высокого уровня. Применение декомпиляторов к исследуемому ПО реализует **статический анализ алгоритмов СЗПО по исходному коду.**

Большинство существующих современных декомпиляторов ориентировано на обработку объектных модулей, написанных на языках интерпретирующего типа (FoxPro, Clipper, Visual Basic, Java), декомпиляторы для языков компилирующего типа встречаются крайне редко и обладают ограниченными возможностями в силу технических особенностей процесса компиляции.

Декомпиляция ПО дает доступ к его исходному коду (или его эквиваленту) и позволяет полностью распоряжаться программным продуктом, включая внесение в него функциональных изменений и повторную компиляцию.

17. Средства отладки объектных модулей (Debuggers)

В состав стандартных функций отладчиков входят возможности пошагового выполнения объектного кода, установки точек останова (в т.ч. срабатывающих по условию), просмотра объектного кода ПО в дизассемблированном виде, изменения последовательности выполнения объектного кода, редактирования памяти отлаживаемого процесса, отслеживания изменения данных процесса и др.

В рамках исследования СЗПО использование отладчиков реализует ***динамический анализ алгоритмов СЗПО.*** Преодоление практически любой СЗПО в большинстве случаев невозможно без использования отладочных средств. При этом большая часть отладочных функций реализуется в архитектуре центрального процессора ЭВМ.

18. Средства поиска и замены текстовых и двоичных последовательностей в текстовых и двоичных файлах (Patchers/Hex-editors)

Функционально такие программные средства предназначены для оперативного и простого внесения желаемых изменений в один файл или группу файлов. Многие подобные средства могут производить поиск по заданной маске.

При помощи средств поиска и замены выполняется ***статическая модификация кода СЗПО.*** Как правило, модификация СЗПО с целью лишения ее функциональности состоит в замене нескольких байт объектного кода. В то же время существуют СЗПО, для дезактивации которых требуется модификация большого числа (иногда непостоянных) последовательностей байт, что становится возможным при использовании этого типа программ.

19. Средства редактирования "ресурсов" объектных модулей (Resource Editors)

Подобные программы используются для редактирования текстовых, диа-

логовых, графических, аудио-, видео- и других ресурсов, содержащихся в области данных объектных модулей ПО. В рамках исследования СЗПО подобные средства позволяют производить ***редактирование ресурсов СЗПО.***

Как правило, содержимое всех пунктов меню интерфейса программы, все текстовые сообщения и диалоги, выдаваемые программой, графические элементы интерфейса и др. содержатся в секции ресурсов области данных объектного модуля. Модификация этих ресурсов позволяет изменить интерфейс программы, в том числе активировать отключенные в рамках данной лицензии на ПО пункты меню, предотвратить выдачу приложением предупреждающих надписей о необходимости приобретения ПО, изменить диалоги и т.п. Иногда в текстовых ресурсах содержатся пароли/серийные номера защищенного ПО.

20. Средства загрузки объектных модулей и/или их динамической модификации в ОЗУ (Loaders/In-memory Patchers)

Этот тип программных средств предназначен для модификации памяти процесса ОС во время его выполнения в ОЗУ. За исключением особенностей модификации объектного кода в оперативной памяти, данные средства функционально подобны средствам поиска и замены в файлах.

При помощи таких программ осуществляется **динамическая модификация кода СЗПО.**

Обычно средства динамической модификации кода используются при высокой сложности или нерациональности распаковки/дешифрации объектных модулей защищенного ПО.

21. Средства загрузки и/или модификации контекста объектных модулей в регистрах ЦП

Этот тип программных средств предназначен для изменения состояния регистров центрального процессора ЭВМ во время выполнения определенного объектного модуля ПО. Данные средства реализуют ***изменение контекста процесса выполняемой СЗПО.***

При помощи подобных средств возможно влиять на процесс выполнения объектного кода, не внося в него изменений. С юридической точки зрения, подобное управление центральным процессором не нарушает (да и не может нарушить) никаких законодательных норм, так как оно никак не затрагивает объектный код защищенного ПО, в то же время совершенно аналогичные действия являются составной частью работы ОС.

22. Программы симуляции аппаратных средств (ГМД, ОД, электронных ключей, ЛВС) (FDD/CD/LPT/Network Emulators)

Программы симуляции аппаратных средств предназначены для создания виртуальных устройств, необходимых для функционирования ПО типов, а также обеспечения доступа к ним как к реальной аппаратуре.

Применение подобного ПО к защищенным программным продуктам делает возможным преодоление: ***СЗПО от копирования, СЗПО с электронными ключами, СЗПО с ключевыми дисками, СЗПО с "привязкой" к ЭВМ пользователя и СЗПО с ключевыми файлами и парольных СЗПО с авторизацией через сеть.*** Использование данного типа ПО также является совершенно легальным.

23. Средства симуляции центрального процессора и подпрограмм ОС (CPU/API Emulators)

Программы указанного типа производят виртуализацию центрального процессора ЭВМ и/или определенных функций ОС на время выполнения одного или группы приложений.

Данные средства реализуют ***изменение процесса выполняемой СЗПО.*** Симуляторы процессора или сервисов ОС производят предварительный анализ инструкций процессора или вызовов функций операционной системы и затем обрабатывают и выполняют (или игнорируют) их в соответствии с заложенными заранее правилами.

24. Средства симуляции операционных систем или ЭВМ целиком (OS/PC/Mac/... Emulators)

ПО этого типа предназначено для обеспечения выполнения приложений, созданных для одной программной/аппаратной платформы, на другой платформе. Большая часть подобных программ предоставляет также и отладочные возможности (сопоставимые с возможностями аппаратной отладки, а иногда и превосходящие их по функциональности).

Применение указанного типа программных средств к защищенному ПО ***позволяет осуществлять преодоление СЗПО произвольного типа.***

Симуляторы ОС производят динамический анализ вызовов системных функций обрабатываемого приложения, их конверсию в вызовы текущей ОС и обратную конверсию кодов возврата в коды симулируемой ОС. Симуляторы процессоров делают то же самое, но на уровне машинного кода процессоров.

Несмотря на совершенно "мирные" цели, заключающиеся в обеспечении переносимости приложений между различными платформами, нестандартное использование средств этого типа позволяет преодолевать не только системы защиты программного обеспечения, но и схемы "управления цифровыми правами" (Digital Rights Management) на доступ к авторским произведениям, основанные на "привязке" к ЭВМ пользователя.

25. Средства пакетной обработки команд (Batch Processors/Script Engines)

Данный тип программных средств позволяет выполнять (последовательно или параллельно) сразу целый набор команд, предварительно заданный пользователем. В рамках пакетов заданий поддерживаются операторы цикла и ветвления. Подобные средства позволяют осуществлять ***создание виртуального окружения на время работы СЗПО.***

Условно бесплатные ППр доступны для использования до их приобретения как такового. Как правило, такие продукты содержат ограничения по времени их использования, числу запусков либо функциональному наполнению. При помощи средств пакетной обработки команд возможно создание необходимого программного окружения (установка системной даты, изменение файлов данных СЗПО, изменение параметров ОС и др.) до запуска защищенного ПО с возможностью возврата к предыдущему состоянию окружения по завершении работы ППр.

26. Средства криптоанализа (Password Crackers/Bruteforcers)

Указанный тип программных средств предназначен для анализа и преодоления систем криптографического закрытия информации. Обычно в них реализуется несколько видов атак на шифры: атака с использованием известного открытого текста, исчерпы-

вающий перебор, направленный перебор с эвристикой, перебор по словарю. Используя подобные средства, можно производить ***криптоанализ СЗПО с шифрацией и парольных СЗПО.***

Так как объектные модули ПО состоят из инструкций машинного кода и последовательность таких инструкций иногда возможно предугадать, в ряде случаев возможно произвести атаку по известному открытому тексту, а также ряд других атак для преодоления СЗПО, использующих методы шифрации.

27. Средства генерации паролей и серийных ключей (Key Generators)

Средства подобного типа используются для генерации ключевых последовательностей, удовлетворяющих критериям используемых в СЗПО криптоалгоритмов. Указанный тип средств реализует ***преодоление парольных СЗПО, а также СЗПО с электронными ключами и ключевыми файлами.***

Программы-генераторы различных ключей, кодов возврата и т.п., как правило, являются результатом предварительно проведенного криптоанализа СЗПО и позволяют получать "подходящие" к СЗПО значения ключей для "легального" отключения СЗПО.

28. Средства ОС по контролю доступа к программам и данным (Access Rights Managers)

Средства обеспечения контроля и разделения доступа к данным и приложениям являются одной из основополагающих частей системы безопасности ОС. Данный тип программных средств, как правило, основывается на так называемой "матрице доступа", создаваемой администратором системы. Эта матрица содержит права на доступ к системным ресурсам различных категорий пользователей и прикладных программ (то есть пользователь трактуется как один из процессов ОС).

Применение подобных средств к защищенному ПО реализует ***системный мониторинг СЗПО***. В частности, в ОС Windows NT, например, возможно блокирование доступа к файлам с данными СЗПО или доступа к файлам системной конфигурации (ключам реестра), блокирование созданных СЗПО временных файлов и т.п.

Как уже было отмечено выше, практически все перечисленные программные средства относятся к обычному пользовательскому или системному программному обеспечению. К "незаконным" средствам можно частично отнести лишь средства протоколирования клавиатурного ввода, средства статической модификации файлов и средства генерации серийных номеров ПО. В то же время даже эти типы программных средств способны использоваться (и реально используются) в областях, никак не относящихся к исследованию и преодолению СЗПО и нарушению авторских прав. Средства протоколирования клавиатурного ввода используются для обработки нажатий комбинаций клавиш в рамках функционирования пользовательских интерфейсов ПО, а также систем компьютерного обучения. Кроме того, они могут использоваться для архивирования всей информации, набранной с клавиатуры, с целью восстановления утерянной при сбое информации.

Средства модификации файлов используются в большом количестве областей, например, для оперативной модификации собственных программных проектов, служебных файлов и др.

Средства же генерации ключевых последовательностей могут легально использоваться для восстановления утерянной легальным пользователем ключевой информации (в случае отказа со стороны владельца авторских прав) либо в образовательных целях.

Таким образом, можно утверждать, что необдуманное запрещение использования перечисленных типов ПО (по аналогии с вредоносными программами) будет неэффективной мерой, так как повлечет за собой серьезные трудности либо полную невозможность использования ПО, необходимого для нормального функционирования компьютерных систем. Естественно, подобное запрещение не будет соблюдаться на практике из-за его невыполнимости.

Возможно законодательное запрещение "нецелевого использования" приведенных типов ПО, но на законодательном уровне практически невозможно регламентировать "целевые" и "нецелевые" виды использования ПО, что ведет к практической неприменимости (или высокой сложности и неоднозначности применения) подобных законодательных норм.

Из всего вышеперечисленного можно сделать вывод, что одни только технические меры защиты ПО, даже с учетом их законодательной поддержки, не способны обеспечить надлежащий уровень безопасности защищаемых программных продуктов. Следовательно, необходим более комплексный подход к защите ПО, с учетом многих других аспектов распространения, реализации и использования программного обеспечения.

* * *

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. *Середа С.А. Оценка эффективности систем защиты программного обеспечения. Материалы Международной конференции IPSIT'99, 1999. http://www.security.ase.md/*
2. *Середа С.А. Программно-аппаратные системы защиты программного обеспечения. Материалы Международной конференции аспирантов при Экономической Академии Республики Молдова, 1999. http://www.security.ase.md/*
3. *Материалы узла Fravia's Pages of Reverse Engineering. http://fravia.anticrack.de или http://tsehp.cjb.net*
4. *Защита программного обеспечения. Под ред. Д. Гроувера: Пер с англ. - М., Мир, 1992.*
5. *Сяо Д., Керр Д., Мэдник С. Защита ЭВМ: Пер с англ. - М., Мир, 1982.*
6. *Черней Г.А., Охрименко С.А., Ляху Ф.С. Безопасность автоматизированных информационных систем. - Кишинев, Ruxanda, 1996.*
7. *Гудман С., Хидетниеми С. Введение в разработку и анализ алгоритмов: Пер с англ. - М., Мир, 1981.*
8. *Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. - М., Яхтсмен, 1993.*
9. *Щербаков А. Защита от копирования. - М., ЭДЕЛЬ, 1992.*

* * *