3.5. Средства и методы борьбы с известными злоупотреблениями.

Рассмотрим основные методы и средства борьбы с программными злоупотреблениями и злоупотреблениями, осуществляемых с помощью компьютера.

1. Программы открытия паролей. Для обеспечения защиты от программ открытия паролей необходимо, чтобы блок идентификации и аутентификации запрашивал пароль ограниченное число раз, после чего выдавал сигнал тревоги. Другим методом борьбы является использования “умной” программы запроса паролей (smart password asker) [177]. При этом методе предполагается использование специальной программы запроса паролей, которая работает не по стандартному алгоритму, а по алгоритму с псевдослучайным исходом. Примером может быть случай, когда программа запроса не запрашивает весь пароль, а только часть (например - первая и третья буква, вторая и последняя и т.д.). В подобном случае вероятность открытия пароля многократно уменьшается.

2. Программы захвата паролей. Для борьбы с данным злоупотреблением необходимо ограничить доступ непроверенных программ в компьютер. Другим важным, по нашему мнению, методом является обучение пользователей тому, чтобы в случае непредвиденного сбоя они сразу же вызывали технический персонал (лучше всего системного программиста) для того, чтобы определить причину сбоя. Если используется “умная” программа запроса паролей, то работа программы захвата паролей приостанавливается, т.к. она не сможет получить всю необходимую информацию.

3. “Люки”. При проектировании “сверху-вниз” проверяется функциональная полнота и проводится анализ возможности появления в системе “заглушек”, которые могут быть использованы в качестве “люка”. Другим методом борьбы с подобными злоупотреблениями или упущениями - это проектирование в системе "защиты от дурака". Смысл

этой защиты состоит в том, чтобы гарантированно отсекать вероятность обработки неопределенного ввода информации и разного рода нестандартных ситуаций. Для выявления “люков” в разработанном программном обеспечении следует выполнить: сквозное тестирование исходных текстов программного обеспечения независимыми экспертами по стандартной методике, описанной в [93, 166]; тестирование программного обеспечения в критических режимах эксплуатации с фиксацией и обязательным устранением выявленных отклонений от нормальной работы.

4. Логические бомбы. Для защиты от логических бомб следует использовать такие средства как ревизия, сегментирование, архивирование и др., что обеспечивает своевременную локализацию механизма логической бомбы. Часто используемым путем распространения логических бомб являются компьютерные игры, программы-утилиты и др. Поэтому следует особенно осторожно использовать вновь появившееся программное обеспечение.

5. Троянские кони. Основным методом защиты от данного злоупотребления является создание замкнутой среды исполнения программ в АИС [30]. Желательно также, чтобы привилегированные и непривилегированные пользователи работали с разными копиями одной и той же программы, хранящейся в разных местах. Также должны использоваться и методы защиты описанные в начале данного параграфа, т.к. в случае реализации данного вида злоупотреблений, существовала возможность восстановления нормальной работы системы. Для предотвращения появления “троянских коней” следует покупать программное обеспечение только у официальных дистрибьютеров, что намного уменьшит вероятность появления в АИС данного вида злоупотреблений.

6. Репликаторы. Самый действенный и распространенный способ защиты от репликаторов является введение ограничений для выполняемого программного обеспечения на использование ресурсов

АИС (время работы процессора, количество операций ввода-вывода, объем оперативной памяти, и др.), а также операторским контролем за их исполнением.

7. Программные закладки. Используются две группы методов защиты от данного вида злоупотреблений [135]:

1) группа общих методов защиты, которые включают:

а) контроль целостности системных областей, запускаемых прикладных программ и используемых данных;

б) контроль цепочек прерываний и фильтрация вызовов критических для безопасности системы прерываний;

в) создание безопасной и изолированной операционной среды;

г) предотвращение результирующего воздействия закладки (например, запись на диск только в зашифрованном виде на уровне контроллера либо запрет записи на диск на аппаратном уровне);

2) группа специальных методов выявления программ с потенциально опасными последствиями:

а) поиск фрагментов кода по характерным последовательностям (сигнатурам), свойственным закладкам, или наоборот, разрешение на выполнение или внедрение в цепочку прерываний только программ с известными сигнатурами;

б) поиск критических участков кода методом семантического анализа.

8. Атака "салями". Защита от подобных злоупотреблений обеспечивается за счет целостности и корректности прикладных программ, обрабатывающих счета клиентов, разграничением доступа пользователей АИС к счетам, а также постоянным контролем на предмет утечки сумм.

9. Скрытые каналы. Ввиду специфики их реализации данные злоупотребления очень трудно предотвратить и обнаружить. Отличительной их чертой является то, что они представляет собой сложную, с технической точки зрения задачу, имеют относительно

небольшую пропускную способность и их достаточно трудно организовать. При этом важно иметь ввиду, что наносимый ими в тактическом плане ущерб обычно небольшой [175]. В то же время, наносимый ими ущерб в стратегическом плане может быть весьма существенным. Для предотвращения подобного злоупотребления необходима разработка комплекса мероприятий, охватывающих использование широкого набора технических и программных средств, в описанных в [30,165,163].

10. Компьютерные вирусы. Вопросы защиты информации воспринимается многими специалистами как сугубо специфические, решаемые только с помощью антивирусного программного обеспечения.

На наш взгляд данный подход неадекватен существу проблемы по ряду причин. Во-первых, обеспечение защиты данных и программного обеспечения только от компьютерных вирусов не может считаться всеобъемлющей, поскольку компьютерные вирусы являются составной частью программных злоупотреблений наряду с программами открытия паролей, логическими бомбами, репликаторами и др. Во-вторых, появился новый класс программных злоупотреблений, действия которых не фиксируются программами антивирусной защиты (например, вирусы-невидимки). В-третьих, программные злоупотребления являются основой компьютерных преступлений, получивших широкое распространение в развитых странах.

Следует выделить важный, по нашему мнению, момент отсутствия достоверной информации, которому уделяется недостаточно внимания. Отсутствие статистических данных, характеризующих состав и удельный вес отдельных вирусов, тип поражений, а также экономические потери, не позволяют обоснованно формировать стандарты информационной безопасности и идеологию противостояния программным злоупотреблениям. Только в последнее время специалисты стали большее внимание уделять экономическим потерям от действий вирусов. Так, например, для устранения известного сетевого вируса Р.Морриса,

реализованного в 1988 году, потребовалось около 400 часов машинного времени.

Способность противостояния компьютерным вирусам и программным злоупотреблениям является одной из актуальных проблем защиты информации в одно - и многопользовательских системах и сетях. Несмотря на короткий временной интервал, характеризующий развитие антивирусных средств защиты, в их составе можно выделить несколько групп, приведенных на рис. 27.

Рис. 27. Классификация средств борьбы с компьютерными вирусами

Как видно из приведенного рисунка с точки зрения охвата различают **однонаправленные** и **комплексные**. Первая группа продуктов была характерна для начального этапа развития "компъютерной вирусологии" и реализовала функции защиты по отношению к отдельным вирусам (например, NOBOOT, NOV1701, NOEDDIE и др.). В дальнейшем однонаправленные программы стали

объединяться в комплексные продукты, способные противостоять большему числу вирусов (например, Scan, AIDSTEST, F-PROT и т.д.).

По типу интеграции продукты разделяются на персональные и встраиваемые. Наибольшее распространение получили встраиваемые продукты, поскольку обеспечивают автоматическую проверку драйверов и исполняемых файлов. Неэффективность персональных программ связана прежде всего с недостаточным уровнем подготовки пользователей.

По количеству обслуживаемых пользователей различают одно- и многопользовательские антивирусные средства. С развитием информационых технологий появилась необходимость в разработке антивирусных продуктов для сетевых операционных систем.

С точки зрения выполняемых функций средства борьбы с компьютерными вирусами могут быть следующих вилов [16-18,86 и др.]:

- *детекторы* - программы, позволяющие составить список пораженных программ;
- *фаги* - программы, “выкусывающие” вирус из зараженной программы и тем самым восстанавливающем ее в виде, близком к первоначальному (частный случай фагов - ***полифаги*** - “выкусывают” только те вирусы, информация о которых в них заложена);
- *“сторожи”* - антивирусные программы, которые являются резидентными и контролируют подозрительные действия в запускаемых программах и блокируют их либо “молча”, либо выдавая соответствующее сообщение;
- *программы - ревизоры* - подсчитывают контрольные суммы и другие параметры файлов и сравнивают их с эталонными. Последние обычно хранятся в отдельном файле;
- *программы - “вакцины”* - подобны естественным вакцинам. Они меняют среду функционирования вируса таким образом, что он теряет способность к размножению. Программы - “вакцины” бывают

пассивными (программа, выполняемая в пакетном режиме, которая за один вызов обрабатывает специальным образом один или больше файлов на диске) и *активными* (резидентные программы, действие которых основано на иммитации присутствия вируса в оперативной памяти).

Наиболее простой способ открытия вирусных механизмов состоит *в поиске во всех файлах вложенных текстовых сигнатур*, являющихся их составной частью и используемых для идентификации (сканирование). Это действенный способ безопасного распознавания вирусов, но есть большое количество вирусов, которые не могут быть открыты подобным путем.

Второй способ защиты - *расчет контрольной суммы* (файла, диска), которая проверяется при запуске и сравнивается с первоначальной. Некоторые вирусы способны преодолевать данный механизм защиты в том случае, если антивирусные средства не поддерживают на достаточном уровне расчет и сравнение контрольной суммы. Существует группа вирусов, которые способны поразить саму антивирусную программу и изменить в ней контрольную сумму.

Большое разнообразие персональных компьютеров, использование различных типов процессоров, операционных систем и других элементов информационных технологий, привело к появлению термина "компьютерная платформа". Данный термин приобретает особое значение при рассмотрении проблем, связанных с обеспечением защиты информации от вирусов, поскольку вирусная инфекция одной или нескольких платформ напрямую связана с механизмами контроля доступа, особенностями архитектуры, операционной системой и др.

Проведенный анализ оценки переносимости вирусов между отдельными платформами и операционными системами позволяет сделать следующие выводы:

- отмечается четко выраженная тенденция существования вирусов в рамках связанных платформ, например, DOS, OS/2 или Windows;

- низкая связанность современных компьютерных систем сдерживает создание и развитие полиплатформных или мультисистемных вирусов. Отсутствие совместимости делает необходимыми соответствующие автоматические преобразования в кодах вирусов, а это требует значительных затрат ресурсов. Но подобное положение не может продолжаться бесконечно долго, поскольку развитие систем передачи информации (спутниковая и оптоволоконная связь), приведет к необходимости повышения совместимости;

- развитие новых версий и реализация отдельных платформ и систем подчинено желанию обеспечить совместимость с существующими приложениями. Одновременно с этим отмечается тенденция объединения платформ и систем посредством использования высоких коммуникационных возможностей. Данные тенденции в значительной степени ухудшают устойчивость новых разработок по обеспечению защиты.

11. "Отказ в обслуживании". Для защиты от такого рода злоупотреблений неоходимо обеспечить мониторинг системы на предмет правомочности действий пользователя. Также необходима реализация политики безопасности, при которой субъекты АИС ограничиваются в ресурсах. При использовании всех предоставленых ресурсов процесс просто прекращается.

12. Работа между строк. Для предотвращения такого рода злоупотреблений существует несколько основных методов: предотвращение физического доступа (подключения) к линиям связи (например, когда в качестве канала передачи используется спутниковая связь, подключение практически невозможно); осуществление сеанса связи, используя шифрование передаваемой информации; специального протокола связи, который в разные моменты времени (которые могут в свою очередь определяться по закону псевдослучайных чисел) осуществляет передачу контрольной последовательности символов.

Другим методом является заполнение промежутков между передачами “мусором” - случайными числами, символами и т.д..

13. **Анализ трафика**. Предотвращение данного злоупотребления возможно за счет исключения возможностей физического доступа (подключения) к линиям связи, шифрованию передаваемой информации, специальными протоколами и др.

14. **“Маскарад”**. Для предотвращения такого рода злоупотребелений, которые могут привести к серьезным последствиям, необходимо использовать надежные методы идентификации и аутентификации, блокировку попыток взлома системы с помощью программ открытия паролей или других средств, контроль входов в нее. Также необходимо фиксировать все события, которые могут свидетельствовать о “маскараде” в системном журнале для его последующего анализа. Также желательно не использовать программные продукты, содержащие ошибки, способствующие к благоприятным условиям для осуществления “маскарада”.

15. **"Подкладывание свиньи"**. Такой вид злоупотреблений может быть осуществлен тогда, когда не происходит существенных изменений в порядке приема/передачи информации относительно долгое время, т.е. система приема/передачи находится в статическом состоянии. Это способствует тому, чтонарушитель имеет возможность получить или исследовать процесс осуществления сеансов связи. Поэтому, для предотвращения таких злоупотреблений важно использовать динамичные методы реализации сеансов связи. Например, в порядок приема/передачи данных вводится элемент случайности (для нарушителя) и таким образом уменьшается вероятность реализации такого рода злоупотреблений.

16. **Повторное использование объектов.** Для предотвращения повторного использования объектов и “сборки мусора” используются различные специальные методы и средства. Одним из них может быть специальная утилита, заполняющая нулями те области дискового пространства, которые освобождаются после удаления файлов средствами операционной системы. Другим методом является установление специальных признаков блокам памяти, при использовании которых, отмеченную свободной память нельзя прочесть до тех пор, пока не будет что-то записано на это место.

17. Запуск “воздушного змея. Предотвращение реализации данного злоупотребления требует блокировку перевода сумм денег из одного банка в другой, в условиях, если на момент осуществления приказа о переводе на счете нет такогй суммы денег.

18. Нелегальное распространение, использование и/или изменение программных средств. Под защитой программ от копирования имеется ввиду предотвращение несанкционированного распространения, использование и/или изменение программных средств. В Российской Федерации принят закон “О правовой охране программ для электронных вычислительных машин и баз данных” [72], призванный обеспечить регулирование взаимоотношений при разработке, продаже и/или распространении и использовании программного обеспечения.

При защите от копирования используется система, обеспечивающая выполнение программой своих функций только при опознании некоторого уникального некопируемого элемента. Таким элементом может быть дискета, определенная часть компьютера или его характеристики, или специальное устройство, подключаемое к компьютеру.

Анализируя описанные в публикациях [153,119,120,54,25,74 и др.] средства и механизмы защиты от копирования, можно выделить следующие группы, используемыхе для защиты программ от несанкционированного копирования (рис. 28):

1. Средства собственной защиты, определяющие элементы защиты, которые присущи самому программному обеспечению или сопровождают его продажу и препятствуют незаконным действиям пользователя. Основными такими элементами являются документация, машинный код, сопровождение, ограниченное применение, заказное проектирование и авторское право.

2. З*ащита в составе вычислительной системы* - состояи из:

- защиты магнитных носителей;

- защитных механизмы устройств ВС - это использование характеристик аппаратуры для защиты программ, а именно: специальные диски; специальные процессоры; шифраторы; дешифраторы и др.

- замков защиты - запрещение доступа к программе, если не выполнены некоторые проверки.

- изменении функций - чередование действий или функций системы.

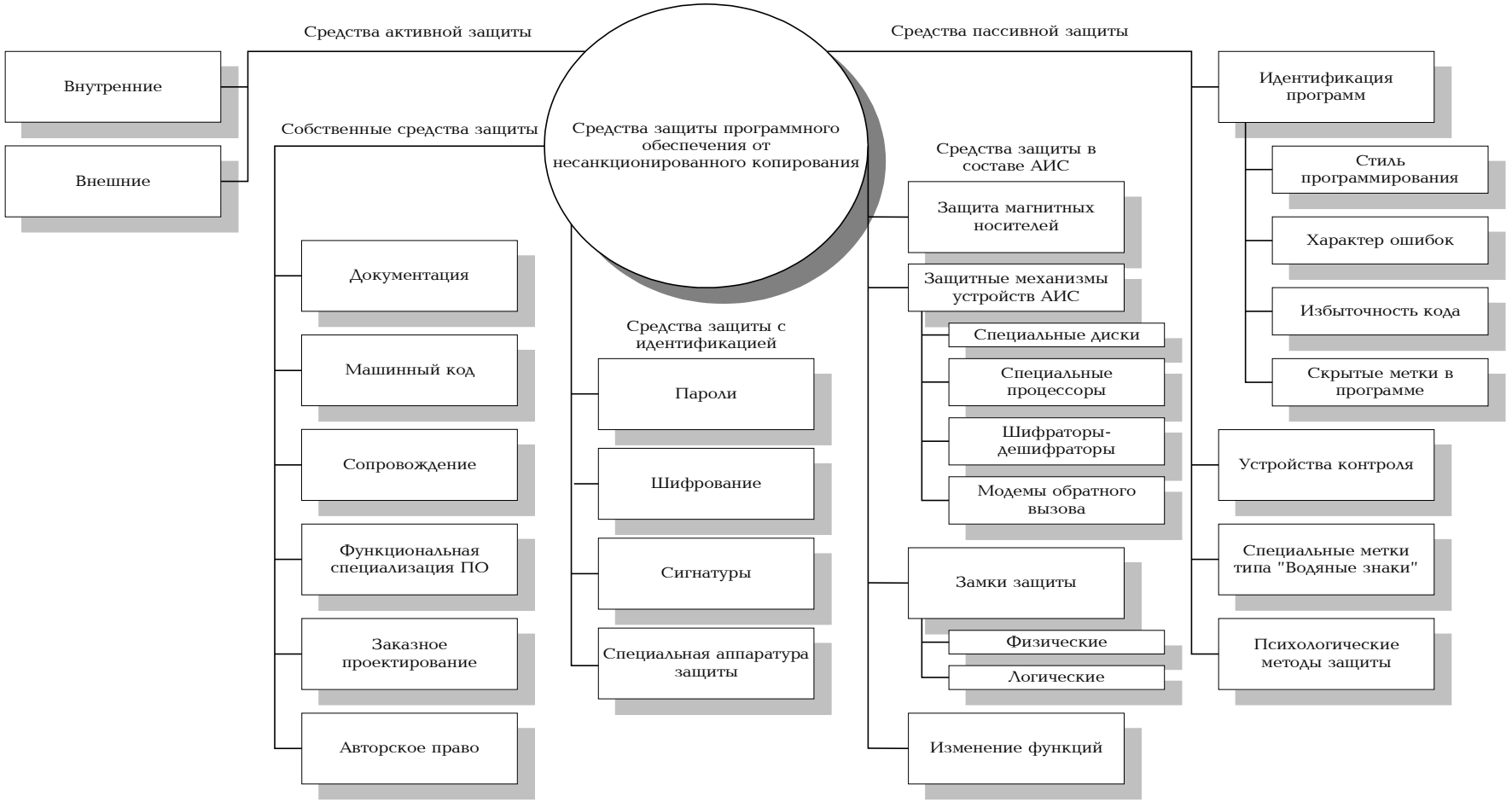

Рис. 28. Классификация методов и средств защиты программного обеспечения от несанкционированного копирования

3. *Средства защиты с запросом информации* - связанные с вводом паролей, сигнатур, ключей и др. Используются следующие основные методы: пароли; шифрование; сигнатуры - уникальная характеристика компьютера или других устройств системы; специальная аппаратура защиты;

4. *Средства активной защиты.* Инициируются при возникновении особых обстоятельств, например при вводе неправильного пароля, идентификатора пользователя и др. подобных условий. Они бывают двух разновидностей:

- внутренние - для автоматического обнаружения и противостояния НСД (блокирование программы, блокирование доступа и т.д.);

- внешние - сигналы тревоги, печать этикетки с авторским правом, напоминания и т.д.

5. *Средства пассивной защиты* - связаны с:

- идентификацией программ по стилю программирования, характеру ошибок, избыточности кода, скрытым меткам в программе и т.д.

- устройства контроля и регистрации событий, процедур и/или доступа к данным;

- водяные знаки, представляющие собой информацию о которой нарушитель знает/или не знает, но не может скопировать.

- психологические методы защиты связанные с созданием у нарушителя чувства неуверенности и психологического напряжения, заставляя его помнить, что в похищении программного продукта могут содержаться средства защиты.

На сегодняшний день существуют два направления эаолюции систем обеспечения защиты от НСК: ***встраиваемые*** (build-in) и ***навешиваемые*** (add-on).

Встраиваемые - это системы, разрабатываемые одновременно с разработкой программного продукта и призванные защитить его от НСК. Обычно они системы обеспечивают лучшую защиту, чем “навешиваемые” системы.

“Навешиваемые” системы защиты от НСК реализованы в виде отдельных программных продуктов. При установке они внедряют себя в

защищаемый программный продукт и активизируются каждый раз, когда запускается защищаемый программный продукт. Нормальная работа с программным продуктом может продолжиться только после опознании системой защиты от НСК некопируемой метки.

В [121] определяются основные требования, выдвигаемые перед системой защиты от несанкционированного копирования. В этой связи механизмы защиты от НСК должны исключить:

* копирование ключевых дискет имеющимися на рынке средствами копирования;

* получение адекватного листинга защитного механизма существующими дизассемблерами;

* исследование работы защитного механизма существующими отладчиками;

* исследование работы защитного механизма с помощью специальных программ типа эмуляторов.

В [120] рассматривается возможная структура механизмов защиты от НСК со следующей структурой:

- блок защиты от раздевателя (БЗОР);
- блок установки характеристик среды (БУХС);
- блок сравнения характеристик среды (БСХС);
- блок ответной реакции (БОР).

По нашему мнению, блок ответной реакции должен отсутствовать, т.к. механизмы ответной реакции могут случайно задействоваться у законного пользователя, что может привести к отказу от пользования программным продуктом. Действие блока ответной реакции может также восприниматься как действие плохо отлаженного участка программы, что опять понизит иммидж программного продукта в глазах пользователей.

В [55] определены основные критерии, которыми следует руководствоваться при выборе системы защиты:

* наиболее мощную и дорогую систему защиты целесообразно использовать лишь в случае единичных поставок дорогого и уникального продукта;

* надежность системы защиты обычно зависит от действия совокупности факторов. К эксплуатационным характеристикам системы защиты, влияющим, прежде всего на ее надежность, можно отнести:

- стабильность и неизменяемость “ключевых” параметров условий окружающей среды, прежде всего при температурных колебаниях;

- устойчивость и возможность противостояния вирусному нападению;

* корректность защиты, выражающаяся в правильности обработки “нестандартных” файлов, прежде всего .EXE, содержащих внутренние оверлеи или подгружаемые данные, .EXE файлов “нового” формата, предназначенные для работы в среде Windows, OS/2 или Presentation Manager;

* размер “вживляемого” модуля не должен превышать 5-10% от объема защищаемой программы;

* удобство процедуры защиты. Программный продукт не будет пользоваться популярностью, если механизм защиты замедляет и/или затрудняет работу;

* защита не должна изменять технологию работы с продуктом, в которой она внедрена;

* возможность реинсталяции защищенной программы;

* соотношение “качество/цена”.

По нашему мнению, требование возможности реинсталяции в определенных условиях, когда “привязка” программного продукта осуществляется по отношению к магнитному носителю, является не положительной, а отрицательной чертой защитного механизма, ибо в условиях, когда распространены современные технические средства, возможно копирование магнитного носителя, на котором инсталирован программный продукт, например, на стриммер, осуществляется деинсталяция, а затем восстановление информации на магнитный носитель типа винчестер.

Расмматривая категорию “качество/цена”, автор не дает определение что понимается под “качеством” и как можно измерять такую величину для определения самого эффективного средства защиты. В [121] развивается идея методов защиты от нелегального копирования и предлагается модель измерения “качества” средства защиты, которая основывается на использовании собранной им статистики.