СОЦИАЛЬНО-ГУМАНИТАРНЫЕ НАУКИ

П.П. Бескид, Т.М. Татарникова

О НЕКОТОРЫХ ПОДХОДАХ К РЕШЕНИЮ ПРОБЛЕМЫ АВТОРСКОГО ПРАВА В СЕТИ ИНТЕРНЕТ

P.P. Beskid, T.M. Tatarnikova

ABOUT SOME APPROACHES TO THE COPYRIGHT SOLUTION OF A PROBLEM IN THE INTERNET

Рассматриваются вопросы защиты авторского права на цифровой контент в глобальной сети Internet. Дается краткая характеристика существующим методам реализации защиты для разного типа контента, таким как шифрование данных, защита носителей информации, электронные ключи защиты, цифровые водяные знаки.

Ключевые слова: авторское право, цифровой контент, защита данных, шифрование данных, аппаратные средства защиты данных, цифровой водяной знак.

Questions of copyright protection to a digital content in global network Internet are considered. The short characteristic is given to existing methods of protection realization for different type of a content, such as data enciphering, protection of data carriers, electronic keys of protection, digital watermarks.

Key words: the copyright, digital content, the data protection, the data enciphering, hardware of the data protection, digital watermark.

В цифровую эру проблема защиты авторского права становится особенно актуальной. Глобальная сеть Интернет насыщена всевозможным контентом: графической, видео-, звуковой информацией. Растет пропускная способность каналов, совершенствуются потоковые технологии. Все аналоговое переводится в цифровое либо сразу производится в цифровом виде. Естественно, что у каждого произведения-творения есть свой автор-правообладатель.

В Законе об авторском праве и смежных правах, который с 01.01.2008 г. действует как ч. 4 ГК РФ, к объектам авторского права отнесены следующие.

1. Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения.

2. Авторское право распространяется как на обнародованные произведения, так и на необнародованные произведения, существующие в какой-либо объективной форме: письменной (рукопись, машинопись, нотная запись и так далее); устной (публичное произнесение, публичное исполнение и так далее); звуко- или видеозаписи (механической, магнитной, цифровой, оптической и так далее); изображения (рисунок, эскиз, картина, план, чертеж, кино-, теле-, видео- или фотокадр и так далее); объемно-пространственной (скульптура, модель, макет, сооружение и так далее); в других формах.

3. Часть произведения (включая его название), которая удовлетворяет требованиям пункта 1 настоящей статьи и может использоваться самостоятельно, является объектом авторского права.

В силу экономических факторов и пренебрежительного отношения к закону массовым тиражом расходятся именно пиратские копии. В сложившейся ситуации для защиты авторских прав законодательных мер явно недостаточно, поэтому авторам, разработчикам и издателям необходимо иметь представление о методах защиты своего контента.

Вопрос о применении и выборе методов защиты требуется рассматривать еще на начальной стадии разработки и создания программ или цифровых произведений. Для защиты цифрового контента применяются:

– шифрование контента и связанной с ним информации;
– защита носителей;
– маркирование информации с помощью цифрового водяного знака, цифровых меток и меток времени;
– аппаратные устройства.

Следует отметить, что надежно защитить интеллектуальную собственность может только комплексное применение различных технологий защиты на различных этапах распространения и использования продукта. Так как разработка собственной технологии защиты – дело сложное и дорогостоящее, лучше воспользоваться готовыми коммерческими решениями или обратиться за советом к специалистам, которые помогут выбрать оптимальный по стоимости и надежности вариант защиты вашего продукта.

Шифрование

Шифрование представляет собой основанный на криптографических алгоритмах способ защиты информации. Под шифрованием понимается процесс преобразования открытых данных в последовательность данных, недоступных для понимания, с помощью некоторого алгоритма (алгоритма шифрования).

При защите цифровых произведений, программ и данных методы шифрования применяются для решения следующих задач:

– обеспечение секретности и конфиденциальности передаваемой информации для предотвращения их незаконного использования;
– обеспечение целостности данных для предотвращения их изменения в процессе передачи;

– идентификация участников финансовых транзакций и пользователей электронного контента;

– применение цифровой подписи для подтверждения подлинности источника информации;

– совместное распространение цифрового контента и информации о способах его использования (цифровых прав);

– подтверждение передачи информации или предоставления услуг.

Существует множество криптографических алгоритмов, которые предоставляют такие возможности. Наиболее известными являются DES, RSA, IDEA, ГОСТ, алгоритм Эль-Гамаля.

Все алгоритмы шифрования базируются на одной из двух схем: шифрование на секретном ключе, базовая модель которой приведена на рис. 1, и шифрование на открытом ключе, базовая модель приведена на рис. 2.

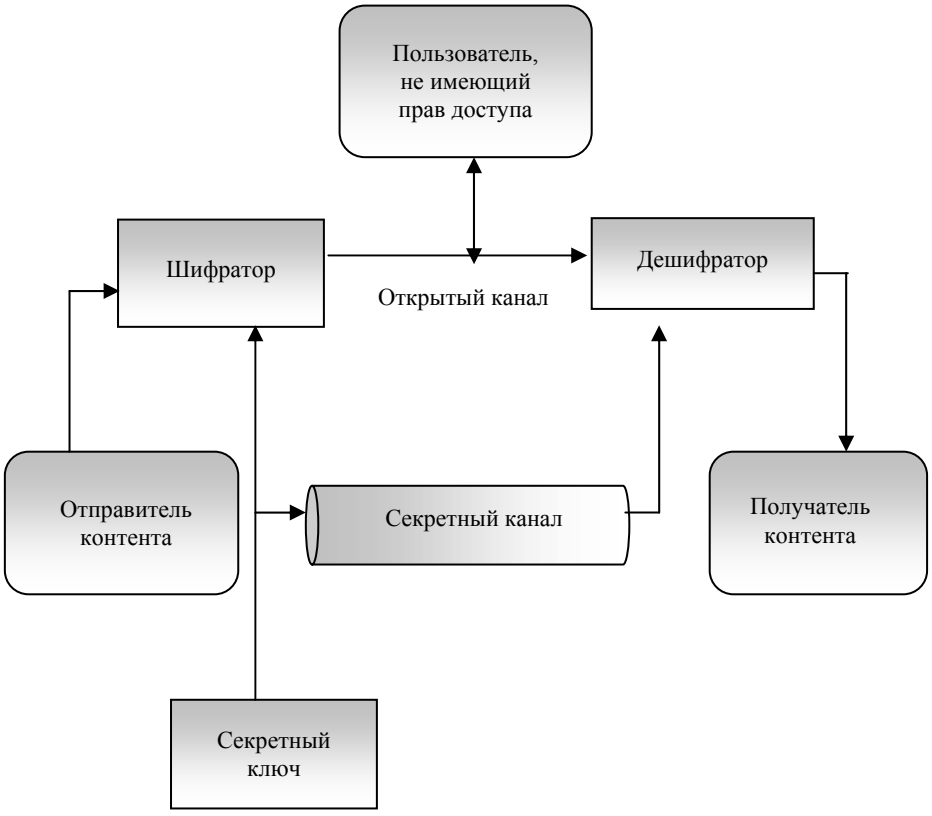

Рис. 1. Одноключевая криптосистема

Автор контента (информационного ресурса) и человек, который хочет воспользоваться этим контентом в своих целях (получить информацию из базы данных, прочесть электронную книгу, скопировать фотографию, скачать музы-

ку и т.д.) должны иметь одинаковые секретные ключи. Процессы шифрования и дешифрования являются симметричными.

В схеме на рис. 2 для шифрования и дешифрования применяются различные ключи. Для шифрования информации, предназначенной конкретному получателю, используют уникальный открытый ключ получателя-адресата.

Соответственно для дешифрования получатель использует парный секретный ключ. Для передачи открытого ключа от получателя к отправителю секретный канал не нужен. Вместо секретного канала используется аутентичный канал, гарантирующий подлинность источника передаваемой информации (открытого ключа отправителя).

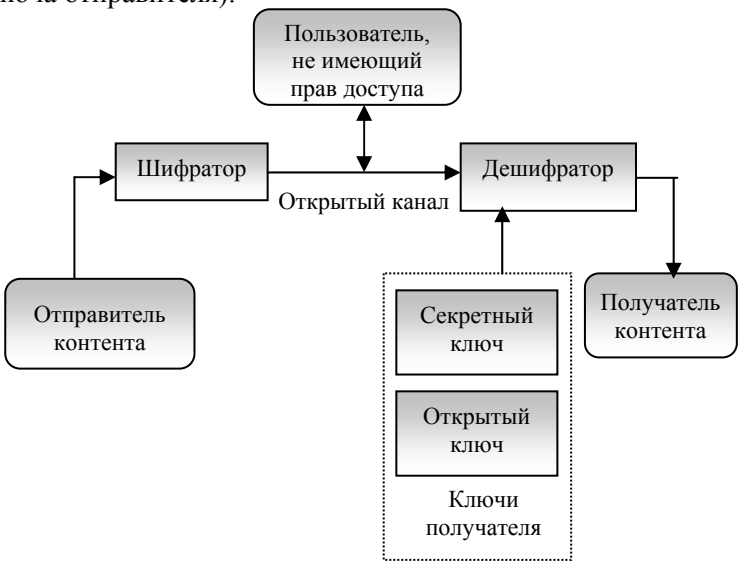

Рис. 2. Двухключевая криптосистема (шифрование/дешифрование)

Защита носителей

Защита носителей производится двумя способами, которые различаются применяемыми технологиями.

Первый способ заключается в том, что на диске участок некоторого файла повреждается аппаратным способом. В процессе работы программа проверяет наличие поврежденного файла и его параметры, после чего делается вывод о легальности копии исполняемой программы. В основном, этот способ применяя-ется для защиты программ и баз данных. Однако этот способ защиты имеет свои недостатки.

Существуют средства, которые могут копировать файлы без поврежденого участка и заменять его некоторой "вставкой". Поэтому иногда используют вариант этого метода, в котором кроме проверки поврежденного файла анализируется также и поверхность носителя на наличие физического дефекта в заданной области.

Второй способ основан на применении одного из вариантов технологии цифрового водяного знака и используется в основном для защиты компакт-дисков. В этом случае на каждый диск записывается некоторая уникальная информация, так называемый электронный отпечаток. В случае обнаружения пиратской копии компакт-диска электронный отпечаток используется для определения авторизованного диска, с которого производилось копирование.

Обычно каждый из этих способов применяется в комплексе с другими методами (шифрование, цифровая подпись и т.п.), что повышает степень защищенности программного обеспечения и цифрового контента.

Электронные ключи

Наряду с программными средствами защиты программ и данных от пиратского копирования и нелегального тиражирования применяются и средства аппаратной защиты.

Наиболее широкое применение среди разработчиков находят электронные ключи.

Электронный ключ представляет собой небольшое микроэлектронное устройство, которое подключается к одному из портов компьютера, и является аппаратным элементом системы защиты приложения.

Электронные ключи собираются на базе специально разрабатываемых для этого микросхем. В настоящее время существуют ключи двух типов:

– на базе микросхем с EEPROM-памятью (EEPROM – Electrically Erasable)

– Programmable Read-Only Memory) на основе ASIC-чипов с памятью или без памяти, которые изготавливаются "под заказ" для каждого разработчика (ASIC – Application Specific Integrated Circuit).

Более совершенные модели ключей имеют энергонезависимую память, в которой храниться служебная информация, необходимая для идентификации самого ключа, разработчика, приложения и его версии. Часть памяти электронного ключа доступна только для чтения, остальная часть доступна для чтения/записи из защищаемого приложения.

В настоящее время возможности технологии электронных ключей настолько широки, что охватывают практически весь спектр способов защиты цифрового контента. Используя электронные ключи, разработчики программ и баз данных, авторы фотографий, аудио- и видео контента могут разрабатывать надежные системы защиты своей интеллектуальной собственности.

Электронный ключ является аппаратным элементом системы защиты приложения и используется для генерации отклика после обращения к нему из программного кода приложения. Обычно применяются два варианта защиты:

– создание защитной оболочки приложения, или так называемого "конверта" (Envelope)

– создание схемы защиты с использованием вызова функций обращения к ключу.

В первом случае защищаются исполняемые файлы уже готового приложения без изменения исходного кода программы. Модуль защиты внедряется в тело программы и при запуске приложения перехватывает управление на себя. При этом он проверяет наличие электронного ключа и соответствие параметров требуемым значениям. В случае положительного ответа защищенная программа загружается, расшифровывается и ей передается управление. В противном случае загрузка и расшифровка программы не производится, и приложение заканчивает выполнение. Недостатком этого варианта защиты является однократная проверка наличия ключа только в момент запуска программы.

Во втором случае для создания системы защиты в исходном коде программмы используются вызовы функций обращения к ключу. Эти функции могут не только проверять наличие ключа, но и осуществлять операции чтения/записи в памяти ключа.

При встраивании функций обращения к ключу в код программы степень защиты приложения значительно возрастает. Однако, чем сложнее проектируемая схема защиты приложения на основе функций обращения к ключу, тем больше усилий и времени придется потратить на разработку и сопровождение программы.

Принцип действия электронных ключей таков (рис. 3).

Рис. 3. Принцип действия электронного ключа

Ключ присоединяется к определённому интерфейсу компьютера. Далее защищённая программа через специальный драйвер отправляет ему запрос, который обрабатывается в соответствии с заданным алгоритмом и возвращается обратно. Вот некоторые характерные запросы:

– проверка наличия подключения ключа;

– считывание с ключа необходимых программе данных в качестве параметра запуска;

– запрос на расшифрование данных или исполняемого кода, необходимых для работы программы (предварительно разработчик защиты шифрует часть кода программы и, понятно, непосредственное выполнение такого зашифрованного кода приводит к ошибке);

– проверка целостности исполняемого кода путём сравнения его текущей контрольной суммы с оригинальной контрольной суммой, считываемой с ключа;

– запрос к встроенным в ключ часам реального времени (при их наличии) и т.д.

Если ответ ключа правильный, то программа продолжает свою работу. В противном случае она может выполнять любые действия, заданные разработчиками – например, переключаться в демонстрационный режим, блокируя доступ к определённым функциям.

Цифровые водяные знаки (ЦВЗ)

Цифровой водяной знак представляет собой некоторую информацию, которая добавляется к цифровому контенту и может быть позднее обнаружена или извлечена для предъявления прав на этот контент. Чаще всего в качестве охраняемого контента на базе технологии ЦВЗ выступают музыкальные произведения, цифровое видео и компьютерная графика.

Теоретическим фундаментом технологии цифрового водяного знака является стеганография – раздел математики, разрабатывающий методы скрытия данных.

Обычно цифровой водяной знак используется в следующих случаях:

– для того чтобы подтвердить право собственности на цифровое произведение;

– для внедрения в каждую копию произведения электронного отпечатка;

– для защиты цифрового контента;

– для идентификации цифрового водяного знака и проверки целостности контента;

– для маркировки цифрового произведения, когда цифровой водяной знак содержит дополнительную информацию о самом произведении.

Существуют различные способы формирования цифрового водяного знака. Они различаются в зависимости от вида контента, маркетинговой политики и каналов распространения. В современных системах формирования цифровых водяных знаков используется принцип встраивания метки, являющейся узкопо-

лосным сигналом, в широком диапазоне частот маркируемого изображения, устойчивым к различным преобразованиям контейнера (атакам). Указанный метод реализуется при помощи двух различных алгоритмов и их возможных модификаций. В первом случае информация скрывается путем фазовой модуляции информационного сигнала (несущей) с псевдослучайной последовательностью чисел. Во втором – имеющийся диапазон частот делится на несколько каналов, и передача производится между этими каналами.

В общем случае типичная схема ЦВЗ выглядит следующим образом (рис. 4).

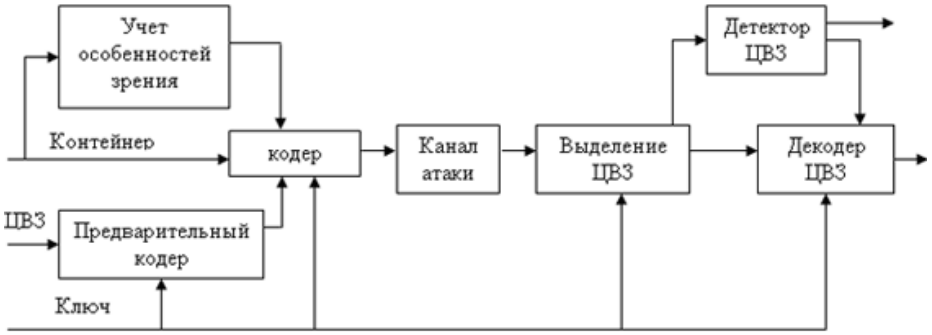

Рис. 4. Схема типичной стегосистемы

Назначение устройств стегосистемы следующее:

– прекодер – устройство, предназначенное для преобразования скрываемого сообщения к виду, удобному для встраивания в сигнал-контейнер (контейнером называется информационная последовательность, в которой прячется сообщение);

– стегокодер – устройство, предназначенное для осуществления вложения скрытого сообщения в другие данные с учетом их модели;

– устройство выделения встроенного сообщения;

– стегодетектор – устройство, предназначенное для определения наличия стегосообщения;

– декодер – устройство, восстанавливающее скрытое сообщение.

Относительно исходного изображения метка является некоторым дополнительным шумом, но так как шум в сигнале присутствует всегда, его незначительное возрастание за счет внедрения метки не дает заметных на глаз искажений. Кроме того, метка рассеивается по всему исходному изображению, в результате чего становится более устойчивой к вырезанию.

Рассмотрим для примера мультикастинговую MPEG-трансляцию. Основная сложность заключается в том, что каждый пользователь должен получать различные копии помеченных данных, с другой стороны задача данной схемы – избежать ретрансляции многочисленных копий.

Основная идея обеспечения защиты для такой трансляции состоит в том, чтобы создать два отмеченных водяными знаками потока, приписать произ-

вольную уникальную последовательность бит каждому пользователю и использовать ее, чтобы разрешить конфликт между двумя помеченными потоками. Перед изложением алгоритма следует подчеркнуть следующие моменты:

– следует использовать необратимую схему добавления цифрового водяного знака. Иначе, такая отметка видеопотока может быть легко дискредитирована;

– различные водяные знаки можно применять для каждого кадра трансляции или один и тот же знак для каждого кадра отдельного потока.

Для простоты рассмотрим второй случай. Детальная схема представлена ниже:

– создаются два потока W_1 и W_2;

– к каждому потоку по необратимой схеме добавляется собственный водяной знак;

– помечается каждый кадр синфазного канала $I_1, I_2,\ldots, I_n$;

– помечается весь видеопоток, используя по отдельности W_1 и W_2. Соответственно на выходе получая результирующие потоки $I_1 + W_0$; $I_2 + W_0$;…; $I_n + W_0$, и $I_1 + W_1$; $I_2 + W_1$; …; $I_n + W_1$;

– создается случайная последовательность бит для каждого пользователя. Длина последовательности равна количеству кадров в потоке. При живой трансляции длина такой последовательности может быть бесконечной;

– для i-го (i = 1,…, количество кадров) помеченного кадра в потоке 0 (в случае двух потоков j = 0 или 1) используется ключ K_{ij} для его кодирования. Потом мы передаем ключ K_{i0} или K_{i1} пользователю n, основываясь на последовательности бит, сгенерированной для этого пользователя. Другими словами, если i-й бит последовательности 0 передаем пользователю n ключ K_{i0}, иначе $_{Ki1}$;

– измененный ключевой заголовок для i-го кадра выглядит следующим образом: $K_{i0}k_1K_{i1}k_2K_{i1}k_3\ldots K_{i0}k_n$

– предполагая, что в i-м бите последовательности стоит 0 для пользователя 1, 1 для пользователя 2, 1 для пользователя 3,…, 0 для пользователя n;

– таким образом, i-й кадр синфазного потока, который подлежит трансляции, имеет следующую структуру: $K_{i0}k_1K_{i1}k_2K_{i1}k_3\ldots K_{i0}k_n\ I_i{+}W_0K_{i0}I_i{+}W_1K_{i1}$

Дадим несколько комментариев к такой схеме.

Во-первых, поскольку для каждого кадра используется новый ключ, то к потоку легко присоединяться и отсоединяться. Эта схема также позволяет легко приостанавливать трансляцию отдельным пользователям и возобновлять ее без перерегистрирования (чтобы исключить пользователя n достаточно не передавать ему новый ключ). Во-вторых, хотя схема не выглядит масштабируемой в соответствии с распределением ключей, она предоставляет оптимизированное решение, благодаря часто меняющимся ключам. С другой стороны, в связи с необходимостью ретранслировать ключи, она оправдана в использовании для трансляций среднего размера (не больше 1000 пользователей). Предположим, каждый ключ состоит из 128 бит или 16 байт, тогда длина ключевого

заголовка составляет 16 000 байт и сравнима с размером одного кадра синфазного потока.

Технология цифрового водяного знака используется обычно совместно с другими методами защиты цифровых произведений. В последнее время она завоевывает все более широкий рынок благодаря своей гибкости и возможности использования новых бизнес-моделей тиражирования и распространения электронного контента.

Среди популярных подходов к решению защиты контента, основанных на перечисленных методах, можно выделить следующие:

– деактивация правой кнопки заключается в отключении функции правой кнопки на большинстве типов мышей и удалении свойства "Сохранить рисунок как", лишая тем самым самого легкого пути получения авторского материала;

– трекинг и удаление – способ, который помогает предотвратить и отследить фото-пиратство, основанный на технологии "водяных знаков";

– Streaming – общепринятый способ защиты записанного видео;

– Digital Rights Management – использование шифрованной лицензии для защиты видео (равно как и другого контента) с различными уровнями защиты. Как только платеж подтвержден, пользователь может просматривать потоковое видео или загружать файл.

Password Protected Streams – парольная защита видео-контента. На фоне стандартных защищенных паролем пакетов, предлагаются также варианты с многократной проверкой авторизации и с маскировкой URL файлов, призванные обезопасить защищенные паролем видео от пиратского копирования.

Выводы

Средства защиты авторских прав среди цифровых источников информации активно развиваются. Совершенствуется и законодательство в этой области. Рынок программных средств защиты интеллектуальной собственности, распространяемой в Интернете и на других цифровых носителях, только складывается. Высоки и рыночные ожидания, хотя в настоящее время определить их трудно. Основная причина в том, что представители индустрии цифровых изображений до сих пор не сформулировали четких критериев оценки существующих коммерческих продуктов и предлагаемых решений по защите авторского права. Очевидно одно – будущее за комплексными решениями.

В настоящее время известны две основные группы методов защиты цифрового контента от атак, это сигнатурные и поведенческие методы. Сигнатурные методы описывают каждую атаку в виде специальной модели или сигнатуры, в качестве которой могут применяться: строка символов, семантическое выражение на специальном языке, формальная математическая модель др. Преимуществом данных методов является высокая точность определения факта атаки, а очевидным недостатком – невозможность обнаружения тех атак, сигнатуры которых пока не определены.

Поведенческие методы базируются не на моделях информационных атак, а на моделях штатного процесса функционирования системы. Принцип работы любого из таких методов основан на обнаружении несоответствия между текущим режимом работы и режимом работы, соответствующим штатной модели данного метода. Любое несоответствие рассматривается как информационная атака. Преимущество методов данного типа – возможность обнаружения новых атак без модификаций или обновлений параметров модели. К сожалению, создать точную модель штатного режима функционирования информационной системы очень сложно.

Одной из наиболее перспективных сигнатурных групп выявления атак являются методы, основанные на биологических моделях. Для их описания используются генетические или нейросетевые алгоритмы.

Нейросетевой метод основан на создании сети взаимосвязанных друг с другом искусственных нейронов, каждый из которых представляет собой пороговый сумматор. После создания нейросеть проходит период «обучения», в течение которого она учится распознавать определенные типы атак: на ее вход подаются данные, являющиеся признаком определённой атаки, после чего параметры нейросети настраиваются таким образом, чтобы на выходе она смогла определить тип этой атаки. Сложность данного метода состоит в том, что необходим чрезвычайно длительный процесс обучения на большом количестве примеров.

На сегодняшний день все методы, базирующиеся на биологических моделях, находятся пока в стадии исследования и широкого коммерческого применения не имеют.

Для моделирования системы обнаружения атак разработана программное обеспечение в среде визуального программирования Delphi, реализующее вероятностную нейронную сеть.

После обучения на вход системы было подано 5 ранее ей неизвестных видов атак на сетевые ресурсы. Результаты распознавания приведены в виде графиков на рис. 1.

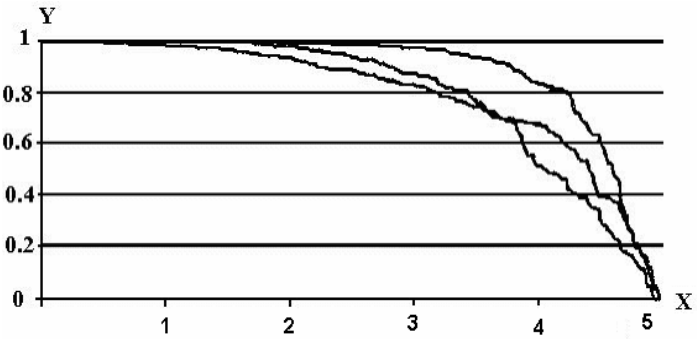

Рис. 1. Вероятность правильного отнесения обнаруженных атак к соответствующему классу атак

По оси *X* отложены номера разных новых атак (всего 5), по оси *Y* – вероятность, с которой они будут отнесены к соответствующему классу атак – на каждый класс реализуется свой метод борьбы – противодействие. Типы атак: 1 – выявление типовых атак Denial of Service; 2 – выявление атак DoS, использующих подмену IP-адреса отправителя (RFC-2827); 3 – выявление класса атак, использующих переполнение буферов; 4 – выявление класса атак, направленных на получение паролей (подбор параметров доступа имя-пароль); 5 – выявление атак уязвимостей протоколов. Для большей наглядности сообщения упорядочены по значениям вероятности. Из графика видно, что правильно классифицировано около 80 % атак на сетевые ресурсы.

Программа зарегистрирована в отраслевом фонде алгоритмов и программ, свидетельство о регистрации № 6078.

Литература

1. *Бохоров К.Ю., Шишко О.В.* Методы и политика в области сохранения произведений медиаискусства. Международной конференции «ЮНЕСКО между двумя этапами Всемирного саммита по информационному обществу» (Санкт-Петербург, Россия, 17–19 мая 2005 г.).
2. *Майстрович Т.В.* Правовые рекомендации для создателей и владельцев электронных библиотек // Рос. ассоц. электр. б-к, Некоммерч. партнерство «Электронные библиотеки»; сост. Т.В. Майстрович [и др.] / Под ред. В.Н. Монахова. – М., 2006. – 188 с.
3. *Судариков С.* Технические меры защиты авторского права и смежных прав // Интеллектуальная собственность. 2001. № 8, с. 44.