Исследование стойкости несетевых электронных изданий и основных видов контента

Б.С. Яковлев, Н.Н. Архангельская,
Н.Е. Проскуряков
Тульский государственный университет
bor_yak@mail.ru

Аннотация

Статья посвящена защите несетевых электронных изданий от несанкционированного доступа. Приведены результаты исследования стойкости популярных форматов электронных книг и контента, входящего в них.
Рассматриваются вопросы стойкости комплексной системы защиты, включая применение физических ключей доступа. Даны рекомендации по повышению стойкости контента и электронных изданий в целом.

Ключевые слова: электронная книга; стойкость форматов; стойкости видов информации; физический ключ доступа; электронная подпись; HASP

1. Актуальность защиты авторских прав и информации в электронных изданиях

Как и любой результат человеческой деятельности, электронные издания нуждаются в защите от несанкционированного использования и копирования. Такая необходимость возникает за счет того, что информационное пространство позволяет относительно легко изъять всю незащищенную информацию в нужной форме без согласия авторов. Особенно остро данная проблема стоит перед образовательными, социально и культурно значимыми проектами, отличающимися от других содержанием разнообразных и уникальных технологий по оформлению самих программных продуктов, представлению материалов и контента [1, 2].

Так же не стоит забывать, что электронные издания все больше стремятся к мультимедиа, т.е отдается предпочтение книгам, содержащим текстовый, графический материал, а также видео, аудио и анимационные вставки. Все эти виды данных создаются различными специалистами, непохожим друг на друга высокоточным, дорогостоящим оборудованием и программным обеспечением, нужны специфические условия съемки, оцифровки данных. Поэтому в сложившейся ситуации целесообразно задуматься о стойкости самих видов информации, в том числе отдельно от оболочки, формата электронных изданий.

Сборник научных статей XVIII Объединенной конференции «Интернет и современное общество» IMS-2015, Санкт-Петербург, 23-25 июня 2015 г.
© Университет ИТМО

В последнее время перед разработчиками из-за большого количества типов мониторов с разными соотношениями сторон появилась новая большая проблема - выбор оптимального метода макетировки изданий. По этой причине появился так называемый математический дизайн. Его суть заключается в том, что все размеры элементов книги, составные части дизайна рассчитываются в зависимости от конкретной ситуации и входных параметров, исходящих от конечного пользователя. Это в свою очередь усложняет процесс создания электронных продуктов. Они более не могут быть сделаны обычным и простым способом - гипертекстовыми, разметочными языками, в них обязаны появиться новые программные подходы, предназначенные для решения подобной задачи.

Все вышеперечисленные факторы усложняют работу над электронными изданиями и удорожают их производство.

По распространенному мнению, наилучшими решениями по защите изданий и контента могут стать применение комплексного подхода к защите информации в электронных изданиях и возможности самих форматов по защите данных. Второй вариант - это обычное паролирование форматов электронных книг, наложение специфических ограничений на работу с контентом, комплексный подход – более сложен и чаще всего заключается в применении программно аппаратной защиты.

Однако, данные методы недостаточно качественно проверялись, им не было уделено должного внимания. Так для разработки и внедрения комплексного подхода необходимо проанализировать эффективность существующих способов защиты информации, выделить факторы, влияющие на стойкость информации к несанкционированному извлечению и копированию.

В настоящее время в системе ГОСТов РФ не существует нормативных документов для электронных изданий и форматов, регламентирующих стойкость. Есть лишь рекомендации от незначительного числа производителей и исследователей стойкости программного обеспечения, баз данных, форматов EXE. Не существует точных предписаний о том, как именно должна защищаться и распространяться информация того или иного рода. По этой причине конкурентная среда производителей и авторов цифрового контента использует самые разные методы защиты прав на свои продукты.

Подобная несогласованность открывает множество возможностей для злоумышленников и в значительной мере обесценивает большинство действий, направленных на защиту интеллектуальной собственности. Существование единых предписаний и рекомендаций по данному вопросу позволило бы существенно повысить степень защищенности цифрового контента и дало бы возможность легко распространять его на условиях производителя или издателя.

В связи с этим перед авторами была поставлена следующая цель: проведение комплексного анализа существующих методов защиты цифровой полиграфической продукции, используемых в большинстве случаев, для выработки рекомендаций по их эффективному применению, а также подтверждения или опровержения имеющихся теоретических положений.

2. Существующие способы защиты, кражи контента и данных из электронных форматов в целом

Графику, так же, как и текстовые данные, очень сложно защитить, так как водяные знаки нецелесообразно ставить по всей площади, это сильно уменьшит читаемость и привлекательность продукта, а одиночные водяные знаки не будут способны к хорошей защите.

Такие методы защиты, однако, применимы к аудио- и видео-форматам. Для их защиты рекомендуют применять наложение фоновых эффектов и помещение в контейнер.

Переходя к защите электронных книг, следует сказать, что злоумышленники давно разработали приложения, способные переконвертировать различные форматы электронных книг, снять защитные механизмы и ограничения, причем ПО стало более универсальным и может быть применимо не к одному виду электронного издания.

Большинство форматов электронных изданий содержит в себе функцию защиты при помощи пароля на открытие, а PDF способен также без запроса пароля ограничивать функционал файла.

EXE-формат считается самым стойким из известных форматов электронных книг, т.к. он полностью преобразует исходный код в машинный, и даже если возможно его частичное восстановление, то графика, находившаяся в EXE-контейнере, пока восстановлению не подлежит. Кроме того, в некоторых компиляторах есть возможность проверки контрольных сумм, что предотвращает редактирование содержимого. Это примитивно, но может отпугнуть злоумышленников.

Следует отметить, что существует большое количество программ и языков, способных к компиляции и единого способа декомпиляции нет [3]. Однако все программы–декомпиляторы работают по похожей схеме: бинарная программа; синтаксический анализатор; семантический анализатор; генератор промежуточного кода; генератор графа потоков управления; анализатор потоков данных; анализатор потоков управления; генератор кода; высокоуровневая программа [3, 4].

Результатом работы таких программ становится некий код, который можно будет скомпилировать вновь и запустить, но данный код не имеет ничего общего с исходным кодом разработчика и часто оказывается неработоспособным [3].

Большинство программистов в процессе создания собственных проектов используют разнообразные динамические библиотеки, которые представляют собой отдельные файлы DLL формата. Такие файлы очень легко вскрыть и извлечь их содержимое, а приложения на их основе не слишком удобны в использовании из-за большого количества файлов. Для решения этой проблемы появился особый класс программ, предназначенных для объединения таких проектов в один исполняемый файл. При этом считается, что происходит оптимизация кода, шифрование данных, однако по сути в результате получается архив, который сначала запускает условное «ядро» и только потом – содержимое хранилища. Этот сегмент развит достаточно плохо, явных лидеров

в этой отрасли сейчас нет. По этой причине использование таких программных продуктов не рекомендуется.

Среди всех известных способов защиты электронных изданий следует выделить комплексный подход. Он наиболее защищен, но и из-за нескольких рубежей защиты он достаточно дорог и поэтому подойдет для разработчика, настроенного на развитие полноценный сети распространения электронных изданий.

Анализируя и обобщая существующие методы защиты данных в электронных изданиях можно сделать вывод, что единственным удачным способом защиты является применение определенных критериев безопасности к контенту, оболочке или типу документа, а также использование программно-аппаратной системы защиты в симбиозе друг с другом. Так, отдельно программная оболочка не сможет обеспечить стойкость видео или звуковых данных, т.к. можно использовать разнообразные внешние устройства, способные эти виды контента оцифровать при просмотре.

Из-за этого необходимо проанализировать стойкость различных видов информации отдельно и в комплексном решении.

3. Исследование стойкости контента, файлов архивного типа и системы комплексной защиты электронных изданий на основе применения физических ключей доступа

Исследование стойкости контента сводилось к попыткам удалить степени защиты, наложенные на тестовые образцы 4 видов данных. Исследованиям подвергались популярные форматы электронных книг, документов, стойкость архивов, в случае их использования для распространения файлов не имеющих своей систему защиты, а также стойкость компилированных электронных изданий и комплексного подхода.

Контент обладал следующими системами защиты: аудио данные – наложение фонового звука, повторяющиеся вставки – звуковые водяные знаки, графические – видимые водяные знаки, текстовые – фоновое изображение на листе, а также без системы защиты, видео – переходы между сценами, и периодические вставки титров и логотипов на прозрачном фоне, случайные по времени вставки титров, а также фоновый звук. Инструментами снятия защиты служили популярные редакторы приведенных выше типов данных: FL-Studio (аудио), Sony Vegas (видео), Fine Reader (текст), Photoshop (графика).

Форматы электронных книг и документов защищались паролями различной длины. Архивные файлы обладали паролем, в образцах были изменены степени сжатия, методы шифрования. Средствами снятия данной защиты служила программа по подбору паролей - Password Recovery Kit Ent 10.3.

Компилированные книги формата EXE защищались физическим ключом доступа, совместимым с программным продуктом Sentinel HASP 5.12 RUS. Анализ производился на основе возможности или невозможности простого изъятия или изменения содержимого программой Restorator.

Текстовую информацию оценивали в зависимости от сложности текста и фонового изображения.

Были взяты по 5 текстов с одинаковым количеством знаков как из художественной, так и научно-технической категорий и проведено их распознавание (см. табл. 1, рис. 1 и 2).

По результатам исследования видно, что наличие в тексте сложных элементов и фонового изображения значительно увеличивает время, необходимое на его распознавание, обработку, и, следовательно, повышает его стойкость.

По результатам исследования заметно, что графическая информация, защищенная сеткой из повторяющихся водяных знаков, требует значительно больше времени на обработку как при помощи инструмента «Штамп», так и при помощи автоматической заливки, что также повышает стойкость такого типа графики.

Создание специализированных IT-структур в системе научно-исследовательских организаций Минздрава началось только с 1975 года. В те годы был учрежден Научный совет по координации НИР и ОКР в области информатизации здравоохранения, запущен республиканский информационно-вычислительный центр Минздрава. К 1980 г. наиболее продвинутые лечебные учреждения довольно масштабно использовали ИТ-системы. Общепринятой методики разработки автоматизированных информационных систем еще не существовало, несмотря на это было построено 11 автономных Медицинских информационных систем, среди которых были Автоматизированный архив, Специализированная реографическая информационная система, информационная система «Ишемическая болезнь сердца», информационная система «Кадры института», информационная система финансовых расчетов и другие, они позволяли решать широкий класс медицинских задач.

На протяжении 1980-х гг. в развитие сети информационно-вычислительных центров продолжилось. К 1991 г. только 10 территорий не имело самостоятельных подразделений информационно-вычислительной службы, парк компьютеров увеличился за 1981–1985 гг. на 237, а в следующую пятилетку уже на 1837ЭВМ.Также успешно велась разработка ПО. Но, несмотря на позитивную динамику, наблюдалась тенденция к выделению информационного обеспечения в несвязанные между собой самостоятельные системы в связи с отсутствием периферийного и сетевого оборудования.[3]

Позже одним из приоритетов государственной политики было обозначено сохранение и укрепление здоровья населения на основе формирования здорового образа жизни и повышения доступности и качества медицинской помощи в целях устойчивого социально-экономического развития России. С 1 января 2006 года стартовал приоритетный национальный проект «Здоровье», представляющий собой программу по повышению качества медицинской помощи, в рамках которого произошло укрепление материально-технической базы лечебно-профилактических учреждений, был решен вопрос оснащенности минимально необходимой вычислительной техникой органов управления здравоохранением.

По итогам заседания президиума Государственного совета Российской Федерации 17 июля 2008 г. и во исполнении поручения Правительства Российской Федерации от 13 августа 2008 г. была разработана Концепция информатизации здравоохранения РФ, в которой освещена необходимость «коренного изменения подхода к информатизации здравоохранения, усиления координирующей роли государства и создания единого информационного пространства в сфере здравоохранения».[1]

В настоящее время система здравоохранения Российской Федерации представляет собой довольно сложную динамическую систему, включающую свыше 17 тыс. поликлиник, около 13 тыс. женских консультаций, кабинетов и детских поликлиник, около 12 тыс. больничных и 700 санаторно-курортных учреждений системы Минздрава России, а также свыше 2,5 тыс. санитарно-эпидемиологических станций, что представлено на рисунке 1.1.1

Качество оказания медицинской помощи можно значительно повысить благодаря совершенствованию информационного обеспечения деятельности медицинских учреждений и фармацевтических организаций, их персонала, студентов медицинских и фармацевтических средних профессиональных и высших учебных заведений, научно-исследовательских организаций. [4]

Для создания здорового общества важным является информирование по вопросам ведения здорового образа жизни, профилактики заболеваний, получения медицинской помощи, качества обслуживания в медицинских организациях.

а)

При осесимметричной схеме операции поле состоит из блока деформаций «1», жестких блоков «2» и «3», разделенных соответствующими поверхностями разрыва скоростей. Инструмент обозначен как блок «0». Для расчета используется верхнеграничная теорема пластичности. Для данной схемы операция она записывается в виде

$$\pi_0\left(r_3^2 - r_1^2\right)V_0 \le N_\partial + N_{12} + N_{13} + N_{mp}. \quad (1)$$

Здесь левая часть – мощность внешних сил; правая – мощности деформаций, мощности на линиях разрыва скоростей и мощность трения. Полагаем, что деформируемому материалу заготовки соответствует уравнение состояния [1, 2]:

$$\sigma_e = A\varepsilon_e^m \xi_e^n, \quad (2)$$

где σ_e, ε_e, ξ_e - соответственно эквивалентные напряжения, деформации и скорости деформаций; A, m, n - константы материала. Уравнение (2) учитывает деформационное и скоростное упрочнение материала.

Рассмотрим объем деформаций. Зададим изменение скорости в нем при перемещении между поверхностями «12» и «13» функцией

$$V = \frac{V_0}{\cos\alpha}\left(1 + \frac{1 - k(y - y_{12})}{y_{12} - y_{13}}\right) = \frac{V_0}{\cos\alpha}\left[1 + \frac{1 - k(y - x \cdot \mathrm{tg}\alpha - r_1)}{(\mathrm{tg}\alpha + \mathrm{ctg}\alpha)x + r_1 - r_3}\right] \quad (3)$$

при граничных условиях, соответствующих плану скоростей (рис. 2):

$$y_{12} = x \cdot \mathrm{tg}\alpha + r_1; \quad V = V_1 = \frac{V_0}{\cos\alpha};$$

$$y_{13} = -x \cdot \mathrm{ctg}\beta + r_3; \quad V = V_3 = V_3 \sin\alpha = \frac{V_0(r_3^2 - r_1^2)}{2hr_3}\sin\alpha.$$

Здесь x, y - произвольные координаты точки в объеме деформаций; y_{12}, y_{13} - уравнения образующих поверхностей разрыва скорости; V_1, V_3 - скорости на входе и выходе из объема деформаций; $k = \frac{r_3^2 - r_1^2}{4hr_3}\sin 2\alpha$.

Рис. 2. План скоростей на линиях разрыва при осесимметричном деформировании

16

б)

Рис. 1. Тестовый объект для текстовой информации (без фонового изображения): а - художественный (простой текст); б - научно-технический (сложный текст)

Таблица 1. Результаты опытов для текстовых данных

Тип контента	Опыт 1	Опыт 2	Опыт 3	Опыт 4	Опыт 5
1. Художественный текст без фона	12 мин.	11,5 мин.	14 мин.	13 мин.	13,3 мин.
2. Художественный текст с фоном	16 мин.	18 мин.	17,2 мин.	20 мин.	17 мин.
3. Технический текст без фона	25 мин.	28 мин.	24 мин.	33 мин.	27,4 мин.
4. Технический текст с фоном	27 мин.	23 мин.	30 мин.	25,6 мин.	26 мин.

Типы графического контента в зависимости от использованного способа защиты можно разделить на простые и сложные. Простыми мы называем изображения, защищенные при помощи единожды встречающегося логотипа, а сложными – изображения, защищенные повторяющимися водяными знаками. Основанием для такого разделения послужило количество времени и усилий, которые необходимо затратить на устранение подобных защитных мер при помощи программных средств (см. рис. 3, табл. 2).

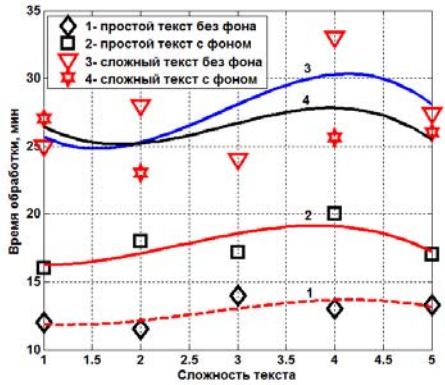

Рис. 2. График обработки текстовой информации

а)

б)

Рис. 3. Тестовый объект для графических объектов:
а - обычное упоминание о правообладателе (простой вариант);
б - сложный водяной знак (сложный вариант)

Таблица 2. Результаты опытов для графических файлов

Тип контента	Опыт 1	Опыт 2	Опыт 3	Опыт 4	Опыт 5
1. Простая система защиты, инструмент Photoshop "Штамп"	0,78 мин.	0,5 мин.	0,4 мин.	0,8 мин.	0,56 мин.
2. Простая система защиты, инструмент Photoshop "Авто-заливка"	1 мин.	1,2 мин.	0,93 мин.	1,1 мин.	1,3 мин.
3. Сложная система защиты, инструмент Photoshop "Штамп"	2,2 мин.	2 мин.	3 мин.	2,8 мин.	3,1 мин.
4. Сложная система защиты, инструмент Photoshop "Авто-заливка"	7,3 мин.	9 мин.	7,6 мин.	8,8 мин.	10 мин.

Также были исследованы три известных способа защиты аудио-контента. В эксперименте участвовали звуковые дорожки, созданные специально для исследования. Самым простым способом защиты подобного контента оказались периодически вставляемые в звуковой ряд аудио-лейблы, которые легко удаляются при помощи обычного монтажа. В этом случае сложность взлома подобной защиты прямо пропорциональна длительности звукового файла, т.к. его необходимо прослушать полностью для выявления всех имеющихся вставок.

Два других способа защиты, среди которых наложение периодического или постоянного звука, мелодии, не удалось преодолеть полностью, т.к. при этом происходило фатальное ухудшение общего качества звучания и по-прежнему оставались фрагменты фоновых записей, занимающие те же частоты, что и оригинальный звук (например, голос диктора).

Видео файлы были разделены на 2 группы сложности: простая - включение уникальных переходов между сценами, помещение графических логотипов поверх проигрываемого видео; сложная - периодическая вставка поверх проигрываемого видео анимированных объектов произвольной формы достаточно большого размера на прозрачном фоне.

Для анализа стойкости видео нами были взяты 5 видеофайлов из каждой группы длительностью по 30 минут и со средним количеством динамичных защитных вставок равным 10, после чего проведена их обработка (см. табл. 3).

Таблица 3. Результаты опытов для видео файлов

Тип контента	Опыт 1	Опыт 2	Опыт 3	Опыт 4	Опыт 5
1. Простая система защиты	13 мин.	17 мин.	12,5 мин.	14 мин.	15 мин.
2. Сложная система защиты	52 мин.	58 мин.	55 мин.	60 мин.	51 мин.

Исследование показало, что обработка видео со сложной системой защиты требует существенно большего количества времени, чем видео с простой системой. Во многом это связано с тем, что расчеты для сложной системы защиты производились с условием необходимости просмотра всей длины видеоролика.

В настоящее время существует универсальный способ защиты, применимый для большого числа форматов. Этот способ представляет собой присвоение файлу пароля. Наиболее часто пароли ставятся на такие форматы как *.doc, *.ppt, *.xls, *.pdf и *.rar. При этом, по распространенному мнению, последний представляет собой один из лучших способов распространения нестойких форматов.

Для проверки этого утверждения мы провели исследование, в ходе которого было использовано программное обеспечение Passware Kit Enterprise. С его помощью были произведены попытки подбора пароля "12w", использованного с файлами различного объема, как в чистом виде, так и помещенными в контейнер RAR.

Для чистоты эксперимента было решено применить методику программного взлома в отношении контейнеров, созданных с различными настройками архивирования. На данном этапе эксперимента каждый раз в контейнер помещался один и тот же файл.

Семейства форматов Microsoft и Adobe были представлены пустыми документами с паролем 12w. Архивный формат был представлен сжатым документом, объемом 976 Кб с тем же паролем на открытие. Результаты экспериментов представлены в табл. 4 и на рис. 1.

Таблица 4. Результаты опытов по стойкости для различных форматов электронных книг

Формат	Опыт 1	Опыт 2	Опыт 3	Опыт 4	Опыт 5
1. *.doc	41 с	41 с	42 с	41 с	42 с
2. *.xls	41 с	41 с	41 с	41 с	41 с
3. *.ppt	41 с	41 с	41 с	41 с	41 с
4. *.pdf	39 с	38 с	39 с	39 с	39 с
5. *.rar	31 с	23 с	23 с	19 с	26 с

По результатам тестов выявилось, что время подбора пароля остается практически неизменным для всех форматов, участвовавших в эксперименте, кроме формата-контейнера *.rar. Время подбора пароля для этого формата несколько меньше, чем для остальных, а серия тестов показала относительную его нестабильность с разрывами между различными попытками более чем в 10 секунд.

Для полноты исследования было решено провести тест с целью узнать, повлияет ли порядок символов (см. табл. 5, рис. 4), количество символов в пароле (см. табл. 6), а также разнородность данных (см. табл. 7), объем (см. табл. 8, рис. 5) и степень сжатия (см. табл. 9) архивного файла на стойкость формата RAR.

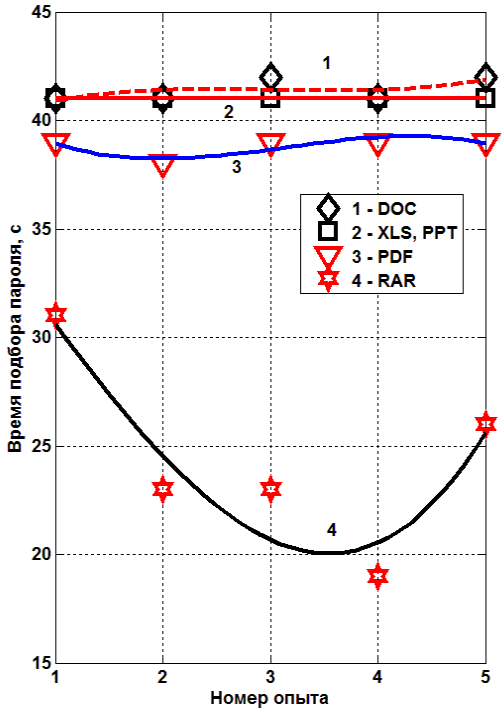

Рис. 4. График подбора паролей для различных форматов электронных документов

Таблица 5. Результаты опытов по стойкости архивных файлов в зависимости от перестановки символов в пароле

Пароль	Опыт 1	Опыт 2	Опыт 3	Опыт 4	Опыт 5
1. 123	1 мин. 42 с	1 мин. 42 с	1 мин. 39 с	1 мин. 41 с	1 мин. 41 с
2. 213	1 мин. 54 с	1 мин. 49 с	1 мин. 50 с	1 мин. 50 с	1 мин. 54 с
3. 312	1 мин. 44 с	1 мин. 46 с	1 мин. 46 с	1 мин. 45 с	1 мин. 46 с
4. 321	1 мин. 39 с	1 мин. 38 с	1 мин. 39 с	1 мин. 40 с	1 мин. 40 с

Таблица 6. Результаты опытов по стойкости архивных файлов в зависимости от количества символов в пароле

Пароль	Опыт 1	Опыт 2	Опыт 3	Опыт 4	Опыт 5
1. 1	1 мин. 9 с	1 мин. 9 с	1 мин. 9 с	1 мин. 9 с	1 мин. 9 с
2. 12	1 мин. 27 с	1 мин. 22 с	1 мин. 22 с	1 мин. 23 с	1 мин. 23 с
3. 123	1 мин. 39 с	1 мин. 39 с	1 мин. 39 с	1 мин. 39 с	1 мин. 39 с
4. 1234	33 мин. 41 с	33 мин. 40 с	33 мин. 41 с	33 мин. 41 с	33 мин. 41 с
5. 12345	>3 ч	>3 ч	>3 ч	>3 ч	>3 ч

Таблица 7. Результаты опытов по стойкости архивных файлов в зависимости от разнородности данных в формате RAR

Описание	Опыт 1	Опыт 2	Опыт 3	Опыт 4	Опыт 5
1. 2 Мб 107 кб, формат doc	32 с	34 с	32 с	36 с	36 с
2. 2 Гб, графические файлы, файлов – 9 218; каталогов– 271	1 мин. 41 с	1 мин. 59 с	1 мин. 42 с	1 мин. 44 с	1 мин. 37 с
3. 3 Гб 433 Мб 45 кб, видеофайл	>2 ч, Неудача	>2 ч, Неудача	>2 ч, Неудача	>2 ч, Неудача	>2 ч, Неудача

Таблица 8. Результаты опытов по стойкости архивных файлов в зависимости от объема файла RAR

Описание	Опыт 1	Опыт 2	Опыт 3	Опыт 4	Опыт 5
1. 500 Мб	36 с	36 с	33 с	35 с	33 с
2. 1 Гб	31 с	36 с	41 с	41 с	39 с
3. 1,5 Гб	27 с	37 с	42 с	40 с	40 с
4. 2 Гб	37 с	37 с	38 с	36 с	37 с
5. 2,5 Гб	43 с	38 с	28 с	38 с	37 с
6. 3 Гб	44 с	39 с	47 с	47 с	42 с
7. 3,5 Гб	36 с	41 с	36 с	43 с	43 с
8. 4 Гб	58 с	42 с	58 с	42 с	45 с

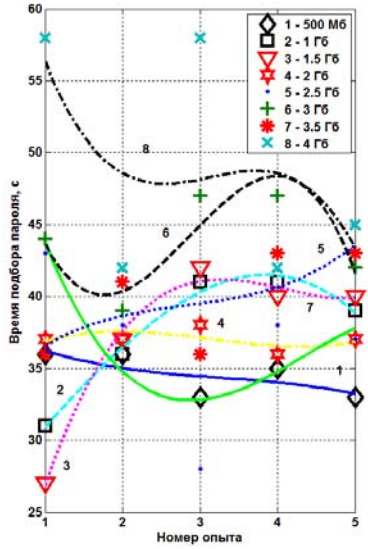

Рис. 5. Влияние разнородности данных в архивном формате на стойкость пароля

Таблица 9. Результаты опытов по стойкости архивных файлов в зависимости от степени сжатия файла RAR

Описание	Опыт 1	Опыт 2	Опыт 3	Опыт 4	Опыт 5
1. Без сжатия	более 2 ч, неудача	более 2 ч, неудача	более 2 ч, неудача	более 2 ч, неудача	более 2 ч, неудача
2. Скоростной	34 с	31 с	33 с	35 с	35 с
3. Быстрый	31 с	31 с	32 с	31 с	31 с
4. Обычный	31 с	31 с	34 с	33 с	32 с
5. Хороший	33 с	26 с	34 с	33 с	36 с
6. Максимальный	26 с	30 с	31 с	30 с	29 с

Защита при помощи компиляторов электронных книг показала хорошую стойкость данных только тех фирм, которые вложили в свои продукты способность проверять контрольные суммы файлов. При помощи программы Restorator (рис. 6) не удалось внедрить в них вредоносный код, либо отдельные файлы. Так же данной программе не удалось найти внутренние ресурсы, только версию компилятора, а также графический символ ярлыка программы и отображение курсора (рис. 6).

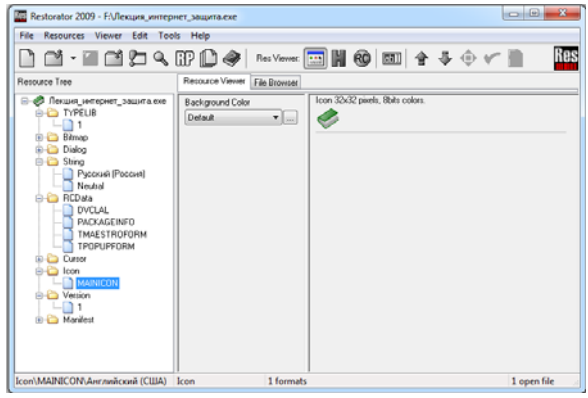

Рис. 6. Результат работы ПО Restorator для компилированных электронных книг без использования физического ключа доступа и технологии HASP

Так же в процессе исследования в нашем распоряжении было два типа ключей: HASP HL drive и Net time. Их принцип работы приведен на рис. 6.

По утверждению разработчиков HASP HL drive является наилучшим решением для распространения объемного ПО. На деле оказалось, что данная технология в операционной системе Windows 7 x64 распозналась как обычная Flash-карта. На нее можно беспрепятственно записывать информацию и копировать ее в обратном направлении без ввода кодов и паролей. Возможно, это связано с тем, что именно эта технология была разработана для более старых операционных систем, но это делает непригодным ее к применению.

Иначе дела обстоят с технологией Net time. Она служит для того, чтобы без использования специального ключа доступа определенная программа не могла

запуститься, однако сам по себе он обладает очень малым объемом памяти и предназначен для хранения только специальных ключей. При помощи ПО Sentinel HASP Envelope 5.11 создаются особые правила запуска для конкретных приложений, которые невозможно будет запустить без наличия вставленного в USB-разъем ключа доступа.

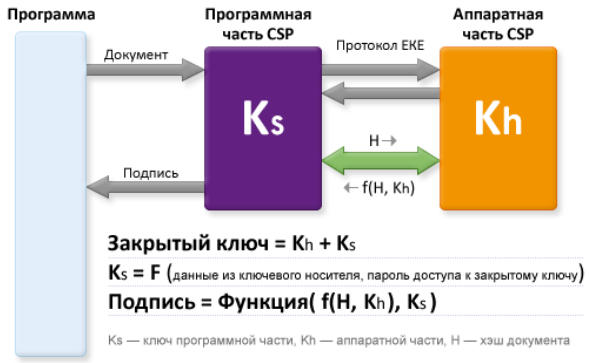

Рис. 7. Общая схема работы физических ключей доступа

По итогу работы ПО Sentinel HASP Envelope программа без ключа доступа не могла запуститься (см. рис. 8), также в ней не было найдено внутренних данных - графики, текста, аудио или видео данных.

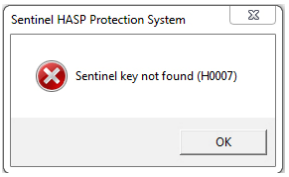

Рис. 8. Результат запуска электронной книги без установленного физического ключа доступа в разъем USB с примененным к ней процедуры шифрования HASP

В данной работе не тестировались технологии облачных сервисов, а также программы, работающие по системе «клиент – сервер». Однако данная тема очень интересна и ее следует развивать как самую перспективную в области «электронной полиграфии». Можно уже сейчас сказать, что по косвенным признакам, технология клиент – серверных приложений более защищена от несанкционированного доступа к своим данным по причине развитого и постоянного мониторинга деятельности конечных пользователей, методов получения информации. Именно постоянное наблюдение за трафиком, а также возможность ввода настраиваемого автоматического анализа деятельности пользователей позволяет быстрее определить, есть ли проблемы с защитой данных, а это уже не мало.

4. Основные выводы и заключение

На основе проведенных исследований были сделаны следующие выводы:

1. Текстовая информация показывает разные результаты стойкости, и ее показатель напрямую связан с типом текста, а также его сложностью.

2. Графические файлы не обладают удовлетворительной стойкостью. Их показатель стойкости напрямую связан с количеством и площадью заполнения видимыми водяными знаками, что отрицательно влияет на художественную ценность иллюстраций книг.

3. Время обработки видеоданных напрямую связано с хронометражем видеофрагмента. В среднем это занимает в 3 раза больше времени, чем общий хронометраж.

4. Для защиты аудио данных электронных книг необходимо применять постоянный фоновый звук, так как его не удается полностью очистить с записи.

5. Часто применяемые в полиграфии форматы показали среднюю стойкость. Проведенный анализ показал, что среди них наибольшей стойкостью обладают файлы корпорации Microsoft, на втором месте находятся файлы самого популярного формата файлов среди полиграфистов и пользователей Интернет - PDF.

6. Архиватор RAR демонстрирует разнонаправленность по подбору паролей, т.к. на его стойкость активно влияют как его содержание, так и степень сжатия, что было выявлено в ходе проведения экспериментов.

7. Проверка времени подбора паролей показала, что на него влияют как длина пароля, так и символы, используемые при его создании, т.е. использование только цифрового пароля, цифро-алфавитного или цифро-алфавитного с внедрением специальных символов. Что подтверждает общую теорию стойкости паролей.

8. Комплексный подход с применением физического ключа доступа NetTime и ПО Sentinel HASP Envelope 5.12 показывают высокую стойкость к взлому или изменению данных в файле типа EXE. После манипуляций с содержимым файлы перестали выполняться.

Общее заключение можно свести к следующему: при коммерческом распространении off-line электронных книг необходимо использовать самодостаточную оболочку, в которой изначальный код и ресурсы преобразуются в машинный код.

Выполненный анализ позволил составить рекомендации производителям электронных книг для обеспечения наилучшего качества защиты:

1. При создании наукоемкой продукции, обладающей различными уникальными функциями (интерактивные обучающие материалы, доступ к сайту ПО и т.д.) стараться выбирать EXE-формат как самый стойкий из существующих в ОС Windows.

2. При написании оболочки электронных книг необходимо внимательно подойти к языку программирования на котором он будет создан. Наилучшим решением будет являться C++.

3. При программировании необходимо использовать нестандартные техники написания алгоритмов: непоследовательно описывать процедуры, избегать применения стандартных инструментов (массивов, сравнений и т.д.), создавать

пустые, ни к чему не ведущие разветвления в алгоритме, чтобы возросло время анализа кода;

4. Для улучшения комплексности защиты нужно применять ПО нескольких фирм производителей, т.е. не использовать одну программу для шифрования, доступа к материалам и т.д. Таким образом, может быть исключен вариант одновременного вскрытия метода защиты.

Литература

[1] Проскуряков Н.Е., Яковлев Б.С. Основные форматы электронных книг и способы их применения / Проскуряков Н.Е., Яковлев Б.С. // Вестник Московского государственного университета печати. Вып. 6, 2010. С. 206–210.

[2] Яковлев Б.С., Проскуряков Н.Е., Панфилов Р.Г. Технологии и тенденции развития электронных изданий // The materials of 7-th Scientific-practical conference «Innovations in publishing, printing and multimedia technologies 2014». Kaunas: Kauno kolegija, 2014. P. 95–102.

[3] Долгова К.Н., Чернов А.В. О некоторых задачах обратной инженерии. Труды Института системного программирования РАН, 2008. Т. 15. С. 119–134.

[4] Щеглов К.Е. Обзор алгоритмов декомпиляции // Электронный журнал «Исследовано в России». URL: http://www.ict.edu.ru/ft/002047/116.pdf (дата обращения 24.03.2014). С. 1143–1158.

Research of resistance of non-network electronic editions and main types of content

B. Yakovlev, N. Arkhangelskaia, N. Proskuriakov
Tula State University

The article is devoted to protection of non-network electronic editions against unauthorized access. Results of research of resistance of popular formats of e-book readers and content of them are given.

The problems of resistance of integrated security system, including the application of physical keys of access are considered. Recommendations to improve the resistance of content and electronic editions in general are made.

Keywords: e-book reader, resistance of formats, resistance of types of information, physical access key, electronic signature, HASP