Новикова Полина Александровна, 9 «А» класс, ГБОУ "Школа с углубленным изучением иностранных языков №1288 им. Героя Советского Союза Н.В.Троян", г. Москва
Руководитель: Красовская Наталья Петровна

Исследование современных методов защиты электронных документов

Проект Новиковой П.А.

9 «а» класс школа №1288

Руководитель: Красовская Н.П.

МОСКВА 2015

ПРОБЛЕМА

Сегодня известно множество методов защиты информации. Какие же методы лучше или хуже? Какие придуманы новые, перспективные? Исследованию этого вопроса и посвящена данная работа.

АКТУАЛЬНОСТЬ

Автоматизация получения, обработки и хранения информации врывается во все сферы нашей жизни. Но как только мы доверили компьютеру вопросы хранения информации, тут же возникает задача ее сохранности. Причем дело не только в вирусах, а и в необходимости ограничивать права доступа к конкретным документам разным группам пользователей или конкретных людей. Поэтому разработка средств защиты электронных документов является очень актуальной в настоящее время.

ОБЪЕКТ ИССЛЕДОВАНИЯ

Рассматриваются различные методы защиты информации и электронных документов.

ПРЕДМЕТ ИССЛЕДОВАНИЯ

Исследуются временные характеристики при использовании различных методов, их сложность для «взломщиков», перспективы и удобство работы с ними.

ЦЕЛЬ

Изучение различных источников информации о методах защиты электронных документов, систематизация методов, выявление слабых и сильных их сторон.

ЗАДАЧИ

Найти и изучить литературные и электронные материалы по данной тематике. Исследовать их с различных точек зрения.

Во все времена главной ценностью являлась информация. Но особое важное значение информация приобрела сегодня – в век сплошной информатизации и компьютеризации. Любой пользователь ЭВМ, будь то частное лицо или сотрудник какой-либо компании, сталкивается с проблемой обеспечения информационной безопасности. Огромное внимание уделяется методам сохранности информации, исключению возможности доступа к ней людей, не имеющих на это прав (злоумышленники, любопытные сотрудники и товарищи, подрядчики, конкуренты).

Существует деление информации по уровню секретности. Признаками секретной информации является наличие, во-первых, законных пользователей которые имеют право владеть этой информацией, во-вторых, незаконных пользователей (нарушителей, противников), стремящихся получить эту информацию, чтобы обратить ее себе во благо и законным пользователям во вред. Для наиболее типичных ситуаций введены даже специальные понятия: государственная тайна, военная тайна, коммерческая тайна, юридическая тайна, врачебная тайна и т. п. [1; 2].

Самым известным и широко используемым методом защиты электронных документов сегодня является использование паролей при входе в компьютер или какую-либо базу данных. Пароль может давать конкретному пользователю все права на владение информацией (чтение, запись, изменение), а может давать комплекс ограниченных прав (например, только чтение). Система паролей пользователей встречается в любой сфере деятельности. Многие создают пароли на своих персональных компьютерах, ноутбуках, смартфонах и т.п.

Пароли можно разделить на несколько типов:

- Символьные - содержащие буквы, цифры и различные символы (. , * ! " # ; ' и т.д.)
- Графические - выбор необходимых для идентификации пользователя графических элементов из предлагаемого набора (по какому-то алгоритму);

- Смешанные - символьный пароль совместно с графическим.

- С «фокусом» - один из вышеперечисленных видов пароля с дополнительным каким-либо действием (например, после ввода пароля необходимо нажать на какую-то конкретную клавишу, переместить курсор в определенное место на экране монитора и т.п.)

Многие пользователи для защиты своих электронных данных выбирают простые, короткие, легко взламываемые пароли, например: используют только цифры или буквы, особенно даты рождения или имена («123», «12052001», «Петя»); последовательность букв, расположенных в ряд на клавиатуре («zxcvbnm»); простое слово или словосочетание («Роза», «Мастер и Маргарита», «password1999»). Обычно это происходит из-за неосведомленности, лени пользователя или объясняется свойствами человеческой памяти, т.к. сложно запомнить стойкий к перебору пароль типа «35xhmGL3$%x39» [3].

Людям очень трудно запомнить последовательность из десяти букв, в то же время им легко запоминать лица людей, места, которые они посетили, или объекты, которые они видели [4]. Поэтому всё большую популярность приобретают графические пароли. Они являются более "дружественными" для человека, и увеличивая уровень безопасности. Разгадывание графического пароля с помощью словаря неосуществимо в принципе, потому что нет никаких словарей для графической информации.

Пароль в подобных системах — это некая графическая картинка. Пользователь должен щёлкнуть мышкой в нескольких точках на этой картинке. Можно загрузить в программу любую фотографию. Главное, она должна обладать следующей особенностью: это должен быть разнообразный по виду пейзаж с множеством «секретных» мест, которые пользователю лично легко запомнить (конкретное дерево, здание, элемент одежды)» [5] (Рис. 1).

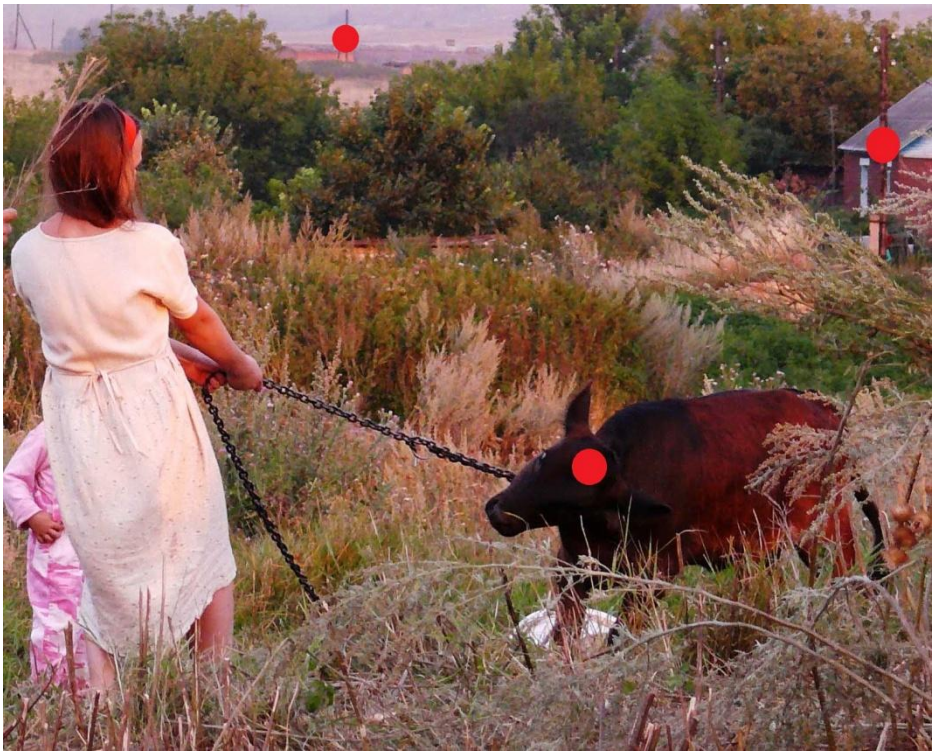

Рисунок 1. Тип графического пароля автора.

Существует и другой способ введения пароля. При создании пароля пользователю предлагается выбрать и запомнить десять иконок примерно из 200-400 возможных. При вводе пароля система выдаёт на экран сразу огромное панно из иконок, перемешанных случайным образом. Среди них обязательно будут три "ваши". Их следует мысленно соединить линиями (получится треугольник) и щёлкнуть мышкой в любой точке внутри этой фигуры» [6] (Рис. 2).

Рисунок 2. Тип графического пароля.

Тут же иконки перестраиваются, перемешиваются. Либо тот же вариант, но с цветными шариками, при этом каждый раз надо щелкнуть на шарике определенного цвета (Рис. 3).

Рисунок 3. Тип графического пароля.

В работе [7] автор предлагают систему нового графического пароля. Пользователю предоставляется несколько коллекций изображений, разбитых по темам. При выборе коллекции появляется поле с девятью изображениями, под которыми располагаются поле для ввода дополнительного текстового пароля и кнопки управления. Пользователь должен выбрать набор изображений и ввести текстовый пароль. При ошибочном вводе пароля изображения перемешиваются, выстраиваясь в новую комбинацию, и текстовое поле очищается. Таких комбинаций девять. Свойство перемешивания изображений позволяет избавиться от «подглядывания» и легкого визуального запоминания пароля со стороны «злоумышленника». В данном случае программа-шпион не сможет отследить ввод графического пароля с клавиатуры, так как клавиатура не используется. И координаты мыши при нажатии на изображения также невозможно отследить, так как изображения перемешиваются, и порядок кликов меняется. Кроме того, можно установить промежуток времени, через который пользователь должен поменять пароль. Запомнить пароль в виде набора картинок легче (например,

вообразив себе некую историю или сценку), в чем и отражается неоспоримое преимущество графических паролей.

Подсчитано, что при длине логина – 6 и 3 знаков, а длине пароля – 8 знаков, нарушитель будет трудиться 123 668 лет и 194 336 лет соответственно (Таблица 1) на подбор пароля:

Таблица 1. Время на взлом пароля

Длина логина	Длина пароля	$T_б$
3	8	123 668 лет
6	8	194 336 лет

Максимальное время на подбор пароля определяется по формуле:

$$T = S^L (D + \frac{C}{R}),$$

где S - это количество символов, включая картинки, из которого выбираются символы пароля (мощность алфавита), L - длина пароля, D - задержка, срабатывающая при вводе неверных реквизитов. Если каждая попытка требует ввода C символов (логин + пароль), а злоумышленник вводит символы со скоростью R знаков в секунду, то на каждую попытку ввода пароля требуется C/R секунд. Если в системе предусмотрена задержка, то величина $(D+C/R)$ определяет полное время, затрачиваемое нарушителем на одну попытку подбора пароля, S^L - общее количество возможных паролей.

Описанная система графического пароля имеет графический блок, содержащий в себе 9 элементов, в которые заносятся изображения из выбранной коллекции изображений. Используем формулу расчета максимального числа комбинаций пароля:

$$A_n^m = \frac{n!}{(n-m)!},$$

где n – алфавит текстового пароля или количество элементов графического пароля; m – количество элементов в водимом пароле.

Получаем:

$$A_9^1 + A_9^2 + A_9^3 + A_9^4 + \ldots + A_9^9 + 1 = 986410$$

т.е. пользователь может выбрать себе пароль из 986 410 комбинаций. В данном расчете не учитывается тот факт, что графический пароль перемешивается.

Если учесть функцию перемешивания графических элементов, то количество комбинаций нажатия элементов будет равным произведению количества всех графических паролей на количество комбинаций последовательности графических элементов, которых в свою очередь 9. Следовательно, количество комбинаций нажатия пароля равно 8 877 681.

Примеры ввода графического и текстового пароля приведен на Рис. 4.

Используя систему графического пароля, можно защитить данные пользователя от их кражи и взлома и хранить пароли в таком виде, что невозможно будет понять и осознать их сущность.

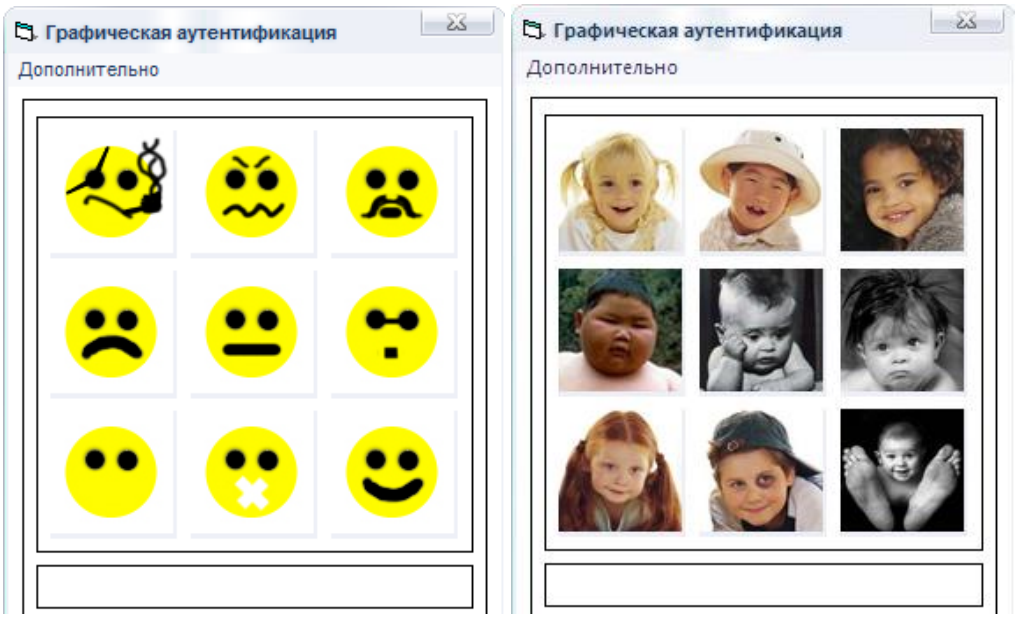

Рисунок 41. Вид формы, заполненной изображениями из коллекции.

Ещё один способ защиты электронных документов от несанкционированного использования - внедрение цифровой подписи. Электронная цифровая подпись (далее просто ЦП) – реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЦП и проверить принадлежность подписи владельцу сертификата ключа ЦП.

Всё большую популярность приобретают алгоритмы внедрения цифровой подписи в неподвижные изображения. При этом ЦП не должна изменять визуального образа подписанного изображения. Подобной подписью могут пользоваться и дизайнеры, и художники, желающие закрепить свое авторство на конкретные изображения, пересылаемые через сеть Интернет. В любой момент можно «выудить» из картинки свой автограф, доказав этим свои авторские права.

Наиболее известные алгоритмы наложения и извлечения ЦП на изображение - алгоритмы Куттера и Брайндокса.

Основой математического описания цвета в цифровых изображениях является экспериментально установленный факт, что любой цвет можно представить в виде смеси определённых количеств трех независимых цветов. Три выбранных цвета называют основными цветами; они определяют

цветовую модель. Тогда любой цвет является смесью трех составляющих основных цветов. Как белый свет является смесью всех цветов радуги.

Для количественного описания цвета предлагается большое количество цветовых координатных систем [8].

Наиболее популярной цветовой системой является модель RGB. В этой модели любой цвет получается как сумма красного, зеленого и синего цветов. Каждый из этих основных цветов имеет значения от 0 до 255 (всего 256 значений). А комбинаций их перемешивания всего 256x256x256=16777216 вариантов. Цветовой куб данной модели представлен на Рис. 5:

Рисунок 5.

Рассмотрим алгоритм Куттера.

Яркость произвольной точки изображения определяется по формуле:

$$Y = 0{,}299R + 0{,}587G + 0{,}114B,$$

где R,G,B – значения основных цветов этой цветовой модели.

Встраивание ЦП выполняется путём изменения яркости в *канал синего цвета*, так как к синему цвету система человеческого зрения наименее

чувствительна и подобные изменения изображения не будут сильно заметны невооруженным глазом: $b` = \begin{cases} b - q * Y, если\ s_i = 1 \\ b + q * Y, если\ s_i = 0 \end{cases}$,

где q - константа, определяющая мощность встраиваемого сигнала, s – индикатор наличия секретной точки. Чем больше q, тем сильнее его заметность.

Алгоритм Брайндокса кратко можно описать так: Изображение разбивается на небольшие блоки. Яркость каждого блока незначительно меняется в соответствии с вводимой цифровой подписью.

Действия алгоритмов Куттера и Брайндокса приведены на Рис. 6.

Рисунок 6. Действия алгоритмов Куттера (слева) и Брайндокса (справа), а также оригинал (снизу).

Большое внимание шифрованию предавал крупнейший французский математик XVI века Франсуа Виет – автор на только замечательного метода решения квадратных уравнений, но и известного Трактата о дешифровании. Секрет успеха Виет видел в методичной и упорядоченной работе. Он советовал систематично искать часто повторяющиеся триады символов, а не пытаться угадать вероятные слова.

При королевском дворе Франсуа Виет проявил себя как талантливый специалист по расшифровке сложных шифров (тайнописи), которыми пользовалась инквизиторская Испания в войне против Франции. Благодаря своему сложному шифру воинствующая Испания могла свободно сноситься с противниками французского короля даже внутри Франции, и эта переписка все время оставалась неразгаданной.

После бесплодных попыток найти к этому шифру ключ Генрих IV обратился, наконец, к Виету с просьбой разгадать тайну шифра. Виет тотчас откликнулся на поручение короля. Он работал дни и ночи в течение двух недель, пока поставленная задача не была решена. Виет разгадал тайну испанского шифра и спас свое отечество от испанских происков. После этого Генрих IV сделал Виета своим личным советником [9].

ВЫВОДЫ

Используя систему графического пароля и цифровой подписи с применением рисунка можно защитить данные пользователя от их кражи и взлома и хранить пароли в таком виде, что невозможно будет понять и осознать их сущность. На мой взгляд, система паролей с использованием изображений наиболее перспективна и получит ближайшее время ещё более бурное развитие, особенно в компьютерных устройствах с сенсорными экранами.

СПИСОК ЛИТЕРАТУРЫ

1. Ященко В. В. Введение в криптографию. М. : МЦНМО: ЧеРо, 1998.

2. Положение о государственной системе защиты информации в РФ от иностранных технических разведок и от ее утечки по техническим каналам //Извлечения.Воениздат. Т.:1993, С. 12.

3. Astera [Электронный ресурс] : Ударим графическим паролем против несанкционированного доступа // Новости ИТ-бизнеса для Профессионалов, 2002, http://www.astera.ru/news/?id=4467.

4. Ваграменко Я. А. Отчет о научно-исследовательской работе "Эргономические требования к экранным элементам управления в программных обучающих и тестирующих комплексах" // Московский Государственный Гуманитарный Университет им М.А. Шолохова, 2001

5. ITnews [Электронный ресурс] : Графические пароли заменят буквенные. ITnews // Новости Информационных Технологий, 2007, http://itnews.com.ua/35750.html.

6. Компьютерра-Онлайн [Электронный ресурс] :«Пароль, который бесполезно подсматривать», 2006, http://www.computerra.ru/focus/256188/.

7. Панкратов Станислав Александрович. Разработка и внедрение комплекса методов автоматизации бизнес-процессов и защиты корпоративного программного и информационного обеспечения производственно-заготовительного предприятия по переработке текстильного вторсырья: автореферат дис. ... кандидата технических наук: 05.13.06. - Москва, 2013

8. Фисенко, В.Т. Компьютерная обработка и распознавание изображений: учеб. Пособие / В.Т. Фисенко, Т.Ю. Фисенко. – СПб: СПбГУ ИТМО, 2008. – 192 с.

9. [Электронный ресурс]: математика для школы, //2014, http://math4school.ru/viete.html