УДК 004.9

Метаданные ФАЙЛОВ - источник угроз национальной безопасности

**Трушин С.М., Зуев А.С.**

Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА — Российский технологический университет», 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: [strmmmrts@gmail.com](mailto:dtghmflysq@gmail.com), [Zuev\_A@mirea.ru](mailto:Zuev_A@mirea.rum)

**Одним из источников утечки информации являются метаданные различных информационных объектов, размещённых в сети Интернет. В данной статье рассматриваются возможные способы получения конфиденциальной информации на основе файлов, находящихся в открытом доступе. При этом собранная информация может являться чувствительной для корпоративной и национальной безопасности. Авторами статьи приводятся метод проверки метаданных объектов и их корректировки.**

Ключевые слова: Метаданные, безопасность, база данных, угроза безопасности.

METADATA FILES A SOURCE OF NATIONAL THREATS

**Trushin S.M., Zuev A.S.**

Federal State Educational Institution of Higher Education “Russian Technological University” (RTU MIREA), 119454, 78 Vernadsky Avenue, Moscow, Russia, e-mail: [strmmmrts@gmail.com](mailto:dtghmflysq@gmail.com), [Zuev\_A@mirea.ru](mailto:Zuev_A@mirea.rum)

**One of the sources of information leakage is metadata of various information objects placed on the Internet.**

**This article discusses possible ways to obtain confidential information based on files that are publicly available.**

**In this case, the information collected may be sensitive to corporate and national security.**

**The authors of the article provide a method for checking the metadata of objects and their correction.**

Keywords: Metadata, security, database, security threat.

Введение

Безопасность в интернете очень важная вещь в наше время, ведь благодаря интернету сейчас осуществляется не один десяток задач, и даже не одна сотня.

Когда-то люди умели хранить секреты. Но с приходом цифровой эры возможностей оставить что-либо конфиденциальным становится все меньше. Данные о наших повседневных действиях: общении с друзьями, поездках в отпуск и покупках — все это и многое другое записывается и хранится на серверах разных компаний и организаций.

Но в наши дни информация не складируется на пыльных носителях где-то в кладовке. Данные хранятся на подключенных к Интернету серверах, их покупают, продают, используют разнообразными способами, а иногда и воруют. И более чем вероятно, что вы не одобрите некоторые сценарии применения ваших данных, если о них узнаете. Всегда неприятно обнаружить, что личные сведения утекли в Сеть и все вокруг обсуждают вашу размолвку с женой, или то, что вы сейчас по уши в долгах, так как вашему ребенку была нужна операция.

Защита личных данных — это важная проблема для людей всех возрастов.

Я предлагаю вам ознакомиться с данной проблемой, а также предложить несколько правил поведения в интернете, которые помогут вам сохранить конфиденциальность.

Метаданные.

Для начала надо разобраться с данным понятием.

Каждая соцсеть — это бесценный источник информации для злоумышленников, собирающих персональные данные, которые они затем используют для обмана и мошенничества. Поэтому так важно правильно настроить конфиденциальность вашего профиля Facebook, «ВКонтакте», «Одноклассников» и любой другой соцсети и не только.

Начнём с простого. Каждая сделанная фотография и выложенная в интернет имеет свои метаданные. Что же это такое? Заглянем на Википедию для объяснения общей характеристики. “ Метаданные — информация о другой информации, или данные, относящиеся к дополнительной информации о содержимом или объекте. Метаданные раскрывают сведения о признаках и свойствах, характеризующих какие-либо сущности, позволяющие автоматически искать и управлять ими в больших информационных потоках.”. Что же это значит? А означает это что при должном умение злоумышленник может узнать о вас почти всё, ведь метаданные существуют не только в фотографиях. Например, посмотрев свойства текстового документа злоумышленник может узнать, начиная от модели устройства, на которое, было сделано и заканчивая вашим адресом и персональным IMEI кодом. Для чего же это нужно? Да много для чего, благодаря этим данным можно узнать ваш логин и пароль. Благодаря найденной информации мы можем составить интернет слепок жертвы. Знать его привычки и любимого питомца. Но не эти ли данные мы вводим как секретный вопрос?

Подытожим про данный способ Пинтесты имитируют известные способы сетевых атак. Успешность теста на проникновения во многом зависит от полноты и качества составления профиля жертвы. Какими сервисами и программами пользуется жертва? На каких протоколах и портах у нее есть открытые подключения? С кем, как, и когда она общается? Почти все это можно получить из открытых источников.

Всем уже наверно интересно что можно найти с помощью этого метода и увидеть его работу.

Приступим к сбору информации. В качестве эксперимента я выбрал Пентагон, да, действительно сайт пентагона, ведь он будет поинтереснее чем чья-то страничка в социальной сети. Это наша учебная цель, о которой мы постараемся накопать как можно больше информации.

Чтобы заняться социальной инженерией, нам потребуется собрать базу почтовых адресов в домене жертвы. Заходим на сайт пентагона и переходим в раздел с контактами.

Видим, что здесь в принципе нет никакой электронной почты. НО мы её найдем. Для этого воспользуемся утилитой theHarvester.

В Kali LINUX эта программа уже есть, я прогнал 500 запросов по всем известным поисковикам, чтобы найти информацию о email. И как не странно - данная утилита свое сделала! Мы нашли 24 почты людей из пентагона, вместо нуля.

Если у них доменная система, а почтовиком назначен сервер Xchange, то есть вероятность что одна из этих найденных электронных почт будет доменной учетной записью.

Теперь обратимся к метаданным. Пентагон должен по любому выкладывать какие-либо документы в открытый доступ их содержимое редко представляет для нас какую-либо ценность, а вот метаданные практически всегда. Как я уже и говорил из них мы можем узнать версию ПО, название учетной записи, название папок или сетевых дисков. С помощью найденных данных мы можем подобрать эксплойты, из них составить список потенциальных логинов взяв из графы автор или определиться с актуальными темами для фишинговой рассылки, так как в некоторых документах указана личная почта и т.д.

Для данных действий нужно собрать как можно больше метаданных, конечно, мы можем сделать это всё ручками, но займёт это очень много времени. Существует много программ для данных операций, но использовать мы будем только ту, которая распространяется открытым способом и не является вредоносным ПО

Далее используем программу FOCA. Потенциал у этой программы намного больше, но мы будем её использовать ради сканирование определенного домена в поиске популярных форматах с помощью трёх поисковиков и с последующим извлечением метаданных

Пентагон оказался полным клондайком для поиска документов так что за одну минуту поисков, из-за большой нагрузки на компьютер пришлось остановить поиск, нашлось около 400 документов (нашлось 361).

Так как скачивание и обработка занимает тоже какое-то количество времени мной был остановлен поиск, так как это мы делаем ради примера, а не для вредоносных атак. Из данной кучи документов я смог узнать:

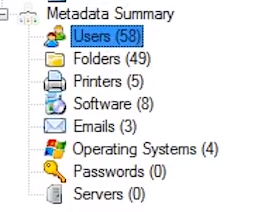


Рис. 1 Найденная информация через приложение FOCA

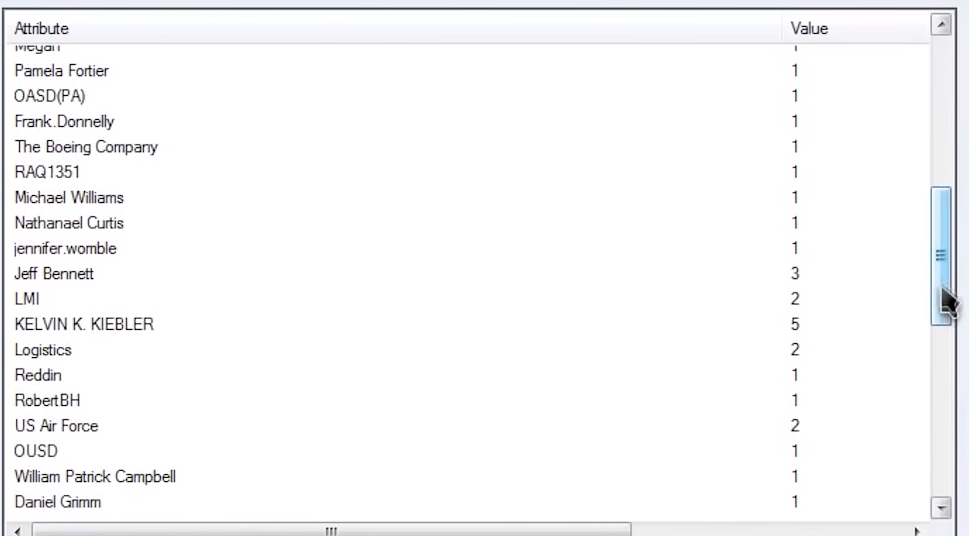


Рис. 2 Найденная информация через приложение FOCA.

1) 58 юзеров, которые чаще всего ставят имя своего же профиля как логин к какой-нибудь информации. Скажем для авторизации в базе данных пентагона.

2) Так же нашлось 49 папок, некоторые из них сетевые жесткие диски.

3) 5 сетевых принтеров

4) 8 программ, точно установленных на компьютерах. Из них можно выявить самые слабые, подверженные той или иной уязвимости, чтобы эксплуатировать при атаках.

5) 3 персональные (не публичные) электронные почты.

6) И 4 компа, с операционной системой. Организации редко проводят апгрэйды, поэтому велика вероятность наличие системы с критическими уязвимостями.

Но это была лишь одна минута тестирования публичной программой, которая нигде не запрещена и это только один из способов получить данные.

Для ещё одного примера можно использовать любую фотографию. Я взял первую попавшуюся фотографию из поисковика. С помощью БЕСПЛАТНОГО, ОТКРЫТОГО, НЕ ЗАПРЕЩЕННОГО сайта я смог узнать вот такие данные.

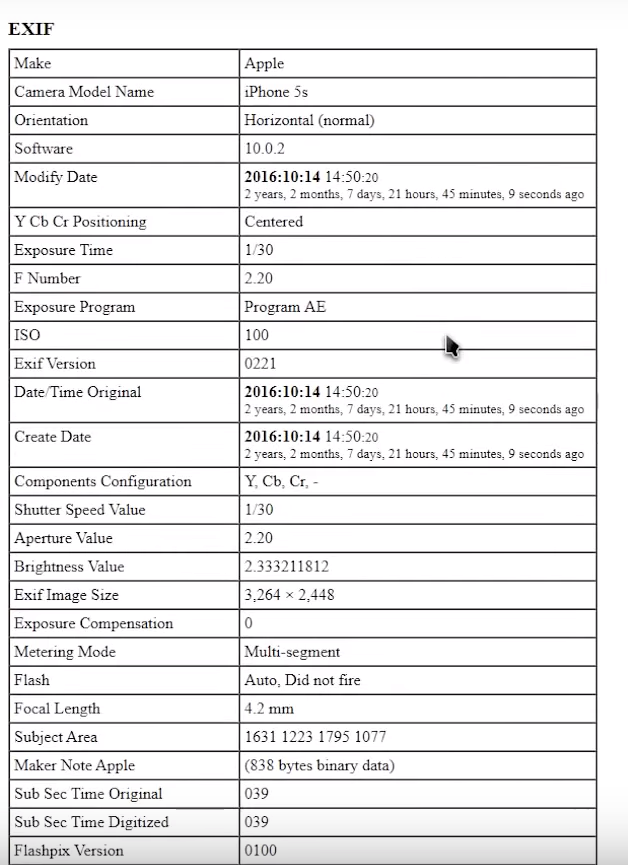


Рис. 3 Сайт для проверки метаданных в фотографиях.

Как и говорилось ранее мы можем посмотреть, где была сделана данная фотография, но для соблюдения конфиденциальности я не буду это показывать.

Теперь займемся получением данных о домене. Для примера возьмем сайт какого-нибудь индийского сообщества.

Мы переходим на сайт Robtex и вводим данные для анализа. Данный сайт может отображать найденную информацию в удобном графическом виде.

Коли я знаю почтовые адреса, то давайте выясним почтовые сервера.

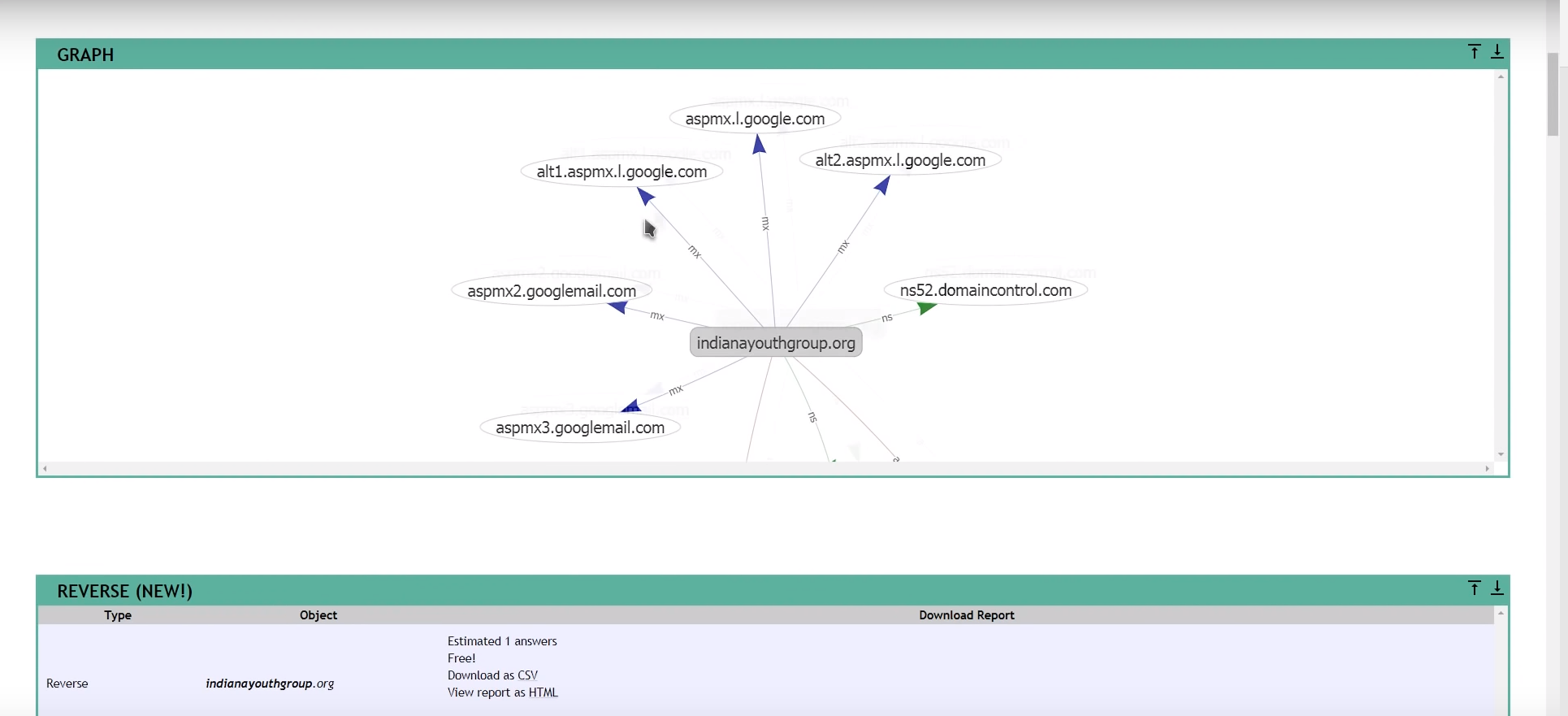


Рис. 4 Главная страница сайта Robtex на примере индийского сообщества. Получение данных почтовых серверов.

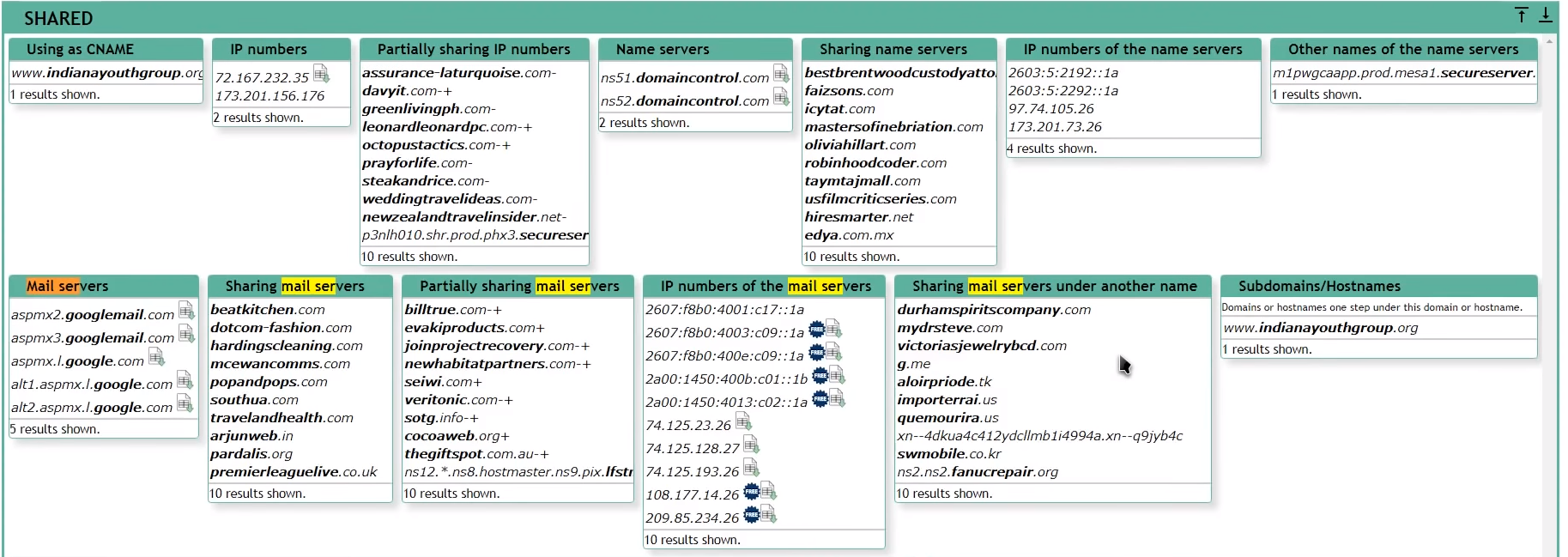


Рис. 5 Главная страница сайта Robtex на примере индийского сообщества. Получение данных почтовых серверов.

Теперь мы можем выяснить DNS сервера этого домена, но исходя из законодательства РФ я не имею права рассказывать, что дальше можно сделать с найденными данными, поэтому я остановлюсь на этом моменте. Но я имею полное право рассказать какие бывают киберпреступления совершенные с помощью найденных метаданных и социальной инженерии.

Метаданные + Соц. Инженерия = ?

Вначале опять же обратимся к википедии для уточнения термина социальная инженерия. Социальная инженерия — это метод управления действиями человека без использования технических средств.

Авторы многих статей на тему социальной инженерии обычно сводят ее применение к звонкам по телефону с целью получения какой-либо конфиденциальной информации (как правило, паролей) посредством выдачи себя за другое лицо. Однако области применения социальной инженерии гораздо шире.

Основные области применения социальной инженерии показаны на рисунке 6.

Но так как мы разговариваем о возможности комбинированной атаке на слабо защищенные данные с помощью соц. Инженерии и метаданных, то и разговор пойдет строго об этом.

С помощью метаданных мы получили множества личных данных, это там нам и было нужно.

На найденную почту может быть отправлено заранее продуманное письмо с вредоносным софтом, или же софт для использования уязвимости в уже найденных программах жертвы. Так как мы нашли личную почту, а не рабочую, то эти мы можем приглушить внимательность человека.

Дальнейшие действия, в целях безопасности, рассказываться не будут.

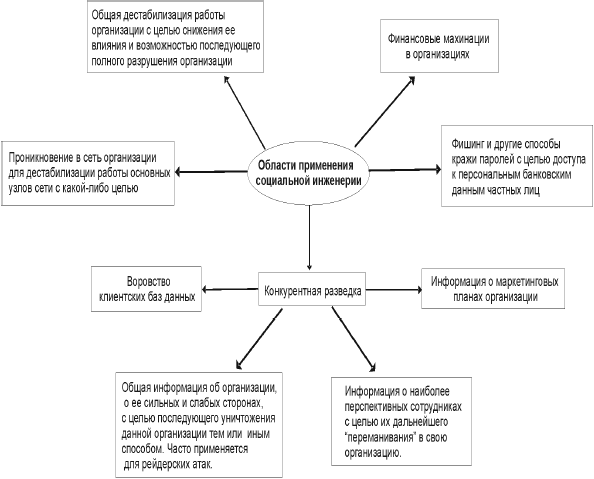


Рис. 6 Основные области применения социальной инженерии.

Как удалить метаданные?

Большинство крупных организаций не задумываются о защите данных и пренебрегают удалением или изменением данных с файлов.

Существует много бесплатного софта для совершения данных действий, но оно оставляет свои следы и тогда преступник сможет это заметить и восстановить оригинальные данных

Для примера разберём ситуацию. Нам нужно удалить метаданные фотографии.

Самый простой способ изменить или удалить метаданные фото — через меню свойства:

1)Нажимаем правой кнопкой мыши и выбираем «Свойства»;

2)Выбираем вкладку «Подробно», далее можем редактировать метаданные, либо удалить их, нажав на ссылку «Удаление свойств и личной информации» и выбрав нужные пункты.

2.1) Изменение и удаление метаданных в свойствах

Но этот способ абсолютно не функционален, так как удалять метаданные из большого количества файлов так никто не будет, кроме того, не всегда можно удалить метаданные в свойствах файла.

Как можно удалить метаданные с помощью Фотошопа?

Удалить метаданные с фото в Фотошопе можно следующим образом:

1)Открыть фото;

2) В меню «Файл» нажать «Сохранить для Web»;

3)При сохранении установить «Не показывать» в пункте «Метаданные»;

3.1) Стереть метаданные в программе Фотошоп;

Существуют сервисы для быстрого удаления метаданных фотографий или видео онлайн без потери качества, и одним из таких сервисов является IMGonline. Чтобы удалить метаданные фото онлайн с помощью данного сервиса необходимо:

1) Нажать на кнопку «Выберите файл»;

2) Выбрать нужный файл с компьютера;

3) Нажать «ОК».

Выводы.

В заключение я хотел бы подытожить полученную и обработанную информацию.

Наш след в интернете позволяет заполучать личные данные, пароли, почты и т.д.. Избавиться от метаданных можно, но не всегда есть возможность это сделать до конца и должным образом, поэтому надо быть осторожнее и всегда смотреть что вы открываете, что вы выкладываете в интернет и на что вы отвечаете.

Для обычного пользователя с его стандартными действиями, для защиты хватит и антивируса, который будет отлавливать большинство хакерских атак.

Список литературы

1. Борисова Д.А., Лядова Л.Н. Иерархическая модель данных как основа реализации информационной системы, управляемой метаданными / 2006. – 4-13 с.

2. Калачев Д.В., Жукова М.Н. О модели системы управления метаданными инцидентов информационной безопасности / Ж. “Актуальные проблемы авиации и космонавтики” 2015. – 491-493 с.

3. Программные средства управления метаданными в процессе разработки и сопровождения базы данных / Ж.: “Вестник пензенского государственного университета”, 2015.- 113-117 с.

References

1. Borisova D.A., Lyadova L.N. Hierarchical data model as the basis for the implementation of the metadata-driven information system / 2006. - 4-13 p.

2. Kalachev D.V., Zhukova M.N. On the model of the information security incident management metadata system / J. “Actual problems of aviation and cosmonautics” 2015. - 491-493 p.

3. Software tools for managing metadata in the process of developing and maintaining a database / J.: “Bulletin of Penza State University”, 2015.- 113-117 p.