Гипермедийные среды и технологии.
Лабораторная работа 4
Совместная работа, авторство, электронная цифровая подпись

Аннотация

Целью данной работы является приобретение теоретических и практических знаний, позволяющих осуществлять совместную работу над гипермедийными документами несколькими лицами, а также осуществлять создание и проверку электронных подписей документов. В ходе работы студент приобретет знания и навыки применения гипермедийных средств в плане совместной деятельности в пакете Microsoft Office, использование криптографических средств на примере GnuPG позволит понять принципы функционирования средств цифровой подписи, а также DRM, которые применяются для защиты авторских прав гипермедийных и иных документов.

Для выполнения лабораторной работы необходимо:

- рабочая станция с установленной ОС Windows XP и более новой (возможен вариант использования терминального доступа),
- приложение GnuPG,
- офисный пакет для создания и обработки файлов формата OOXML: Microsoft Office 2007 SP1 и более новой (возможен вариант использования открытых свободных решений, таких как OpenOffice, LibreOffice и иных).

Терминология

- Коллаборация - совместная деятельность, например, в интеллектуальной сфере, двух и более человек или организаций для достижения общих целей, при которой происходит обмен знаниями, обучение и достижение согласия. Как правило, этот процесс требует наличия руководящего органа, при этом форма руководства может быть и общественной при сотрудничестве равноправных членов децентрализованного сообщества. Считается, что участники коллаборации могут получить больше возможностей достижения успеха в условиях конкуренции за ограниченные ресурсы. Коллаборация может существовать и при противоположности целей, но в этом контексте данное понятие используется редко.
- Системы контроля версий - программное обеспечение для облегчения работы с изменяющейся информацией. Система управления версиями позволяет хранить несколько версий одного и того же документа, при необходимости возвращаться к более ранним версиям, определять, кто и когда сделал то или иное изменение, и многое другое. Такие системы наиболее широко используются при разработке программного обеспечения для хранения исходных кодов разрабатываемой программы. Однако они могут с успехом применяться и в других областях, в которых ведётся работа с большим количеством непрерывно изменяющихся электронных документов. В частности, системы управления версиями применяются в САПР, обычно в составе систем управления данными об изделии (PDM).

Управление версиями используется в инструментах конфигурационного управления.

- Авторское право - в объективном смысле - право, позволяющее регулировать правоотношения, связанные с созданием и использованием (изданием, исполнением, показом и т. д.) произведений науки, литературы или искусства, то есть объективных результатов творческой деятельности людей в этих областях. Программы для ЭВМ и базы данных также охраняются авторским правом. Они приравнены к литературным произведениям и сборникам, соответственно.
- Контрольная сумма (хэш-сумма) – некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении. Также контрольные суммы могут использоваться для быстрого сравнения двух наборов данных на неэквивалентность: с большой вероятностью различные наборы данных будут иметь неравные контрольные суммы. Это может быть использовано, например, для обнаружения компьютерных вирусов. Несмотря на своё название, контрольная сумма не обязательно вычисляется путем суммирования.
- Электронная цифровая подпись (электронная подпись, ЭП, цифровая подпись, ЦП, ЭЦП) - реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).
- Сертификат открытого ключа (сертификат ЭП, сертификат ключа подписи, сертификат ключа проверки электронной подписи (согласно ст. 2 Федерального Закона от 06.04.2011 «Об электронной подписи» № 63-ФЗ)) — электронный или бумажный документ, содержащий открытый ключ, информацию о владельце ключа, области применения ключа, подписанный выдавшим его Удостоверяющим центром и подтверждающий принадлежность открытого ключа владельцу. Открытый ключ может быть использован для организации защищённого канала связи с владельцем двумя способами: - для проверки подписи владельца (аутентификация), - для шифрования посылаемых ему данных (конфиденциальность). Существует две модели организации инфраструктуры сертификатов: централизованная (PKI) и децентрализованная (реализуемая на основе т. н. сетей доверия), получившая наибольшее распространение в сетях PGP.
- Digital rights management (DRM), Технические средства защиты авторских прав (ТСЗАП) - программные или программно-аппаратные средства, которые намеренно ограничивают либо затрудняют различные действия с данными в электронной форме (копирование, модификацию, просмотр и т. п.), либо позволяют отследить такие действия. DRM представляет собой набор систем контроля и управления доступом, а также преднамеренного нарушения авторских прав.

Теория

Понятие совместной работы

В ходе написания документа(-ов), а также написания модулей программного обеспечения часто возникает необходимость оказания или получения помощи от иных лиц, занятых в той же проблемной сфере что и непосредственный автор/редактор документа.

В данном случае файл или пакет файлов, представляющих исходные коды программного обеспечения будем также называть электронными документами или, для простоты, документами.

Документы могут пересылаться при помощи электронных вычислительных сетей, передаваться на переносных накопителях и т.д., то есть могут распространяться между необходимыми получателями. В случае, если конкретный документ передаётся с целью исправления одному лицу, автору не составит труда определить, что было в исходном варианте изменено. Однако если документов много или довольно много получателей, которые позже представят собственную версию документов, вопрос об отслеживании изменений и компоновке изменений в единый готовый пакет встает очень остро.

Для решения данной проблемы при разработке программного обеспечения существует т.н. системы контроля версий (Version Control System, VCS или Revision Control System), которые позволяют отслеживать измененные участки файлов исходного кода, редакторов конкретных участков, компоновать их в единый пакет файлов, а также многое другое.

С точки зрения применяемых технологий, такие системы используют следующие интересующие нас функции:

1. Вычисление «разницы» (diff, difference) между парой конкретных файлов или их частей конкретной ревизии.
2. Удобное отображение «что было – что стало» с возможностью ссылок на конкретные участки текста.
3. Отслеживание авторов, редакторов конкретных участков текста с возможностью просмотра всех изменений, произведенных конкретным автором.

Данные функции имеют важную практическую ценность, а также теоретическую ценность в плане изучения применяемых гипермедийных технологий или **в** гипермедийных технологиях.

В большинстве программных реализаций систем контроля версий, просмотр изменений представляет собой просмотр связей или гиперсвязей, поскольку технологии используются для создания нелинейной среды восприятия информации.

Создание электронных документов, в том числе руководств, также может быть облегчено с использованием систем контроля версий, таким образом, очевидно, что эти системы в том числе также применимы и в издательском деле.

Авторство

Когда кто-либо создаёт документ, который в последствии может быть передан на редактирование или просмотр другим лицам, важно позаботиться о сохранении авторства. В данном случае, принятие и доказательство авторства конкретного субъекта (в нашем случае, документа), позволит не только для подчёркивания самоуважения, в том числе, чувства собственного достоинства (что может быть немаловажно для осуществления продуктивной работы в дальнейшем), но также и для защиты собственных интересов в случае возникновения конфликтных ситуаций.

Фиксация авторских признаков для конкретного субъекта может быть необходима в случае, когда возникают определенного вида споры, например, о первенстве публикации научных открытий и пр.

Стоит отметить, что авторское право является отдельным объектом, защиту которого осуществляет не только сам автор, но и государство в лице уполномоченных органов.

С другой стороны, если автор обеспечит свой результат умственного или ручного труда защитой с точки зрения авторского права, считается дурным тоном, если автор вскоре откажется от своего творения (т.н. принцип «неотказуемости»).

Множество программных продуктов поддерживают возможность фиксации авторских атрибутов для конкретных файлов. Более того, файл – как объект защиты с точки зрения операционной системы обязан иметь автора (логический идентификатор создателя), дату создания и/или изменения и, в некоторых случаях, права доступа к файлу. Прикладные программные продукты, как правило содержат информацию о создателе, редакторе и иных лицах непосредственно в формируемой структуре файла, причем данная информация может отличаться от информации, которую содержит операционная система.

Защита целостности и авторства

Помимо законодательных способов защиты авторства, существуют несколько иных способов защиты электронных «творений» не только от возможности неавторизованной модификации, но и от возможности модификации в принципе.

Представим следующую ситуацию. Некий сотрудник создал электронный документ и должен его передать заказчику. Сотрудник не может напрямую передать документ, поэтому он сперва передаёт документ секретарю для оформления акта передачи. Секретарь, по неизвестной сотруднику причине, модифицировал документ и передал его заказчику, который в последствии остался недоволен внесенными правками (он не знает, что правки внёс секретарь). В данной ситуации виновником вероятнее всего станет сотрудник, который неправильно сформировал документ.

Выход 1 – проверка контрольных сумм.

Перед отправкой документа, сотрудник создает контрольную сумму документа и заносит её в реестр заказчика. Заказчик может проверить контрольную сумму и убедиться, что в процессе передачи файл не модифицировался, НО существует вероятность, что секретарь, знающий об этом механизме может после собственных модификаций пересчитать контрольную сумму и обновить её в реестре, если у него есть доступ.

Выход 2 – шифрование контрольной суммы ассиметричным алгоритмом.

Сотрудник обладает некоторым секретным ключом, который он никому не передаёт, производит подсчёт контрольной суммы документа и позже зашифровывает эту сумму, которую заносит в реестр заказчика. Заказчик, обладающий вторым ключом, называемым «открытым» производит расшифровку суммы, и проверку файла. В случае, если файл модифицировался – заказчик сможет определить, что кто-то, НО не сотрудник модифицировал файл. В случае, если секретарь также знает об этом механизме и обладает собственным закрытым ключом, он может после модификаций поступить аналогично сотруднику, однако заказчик не сможет расшифровать контрольную сумму и снова заподозрит модификацию документа. Если же заказчик обладает также открытым ключом секретаря, ему не составит труда определить, что сумма была пересчитана именно секретарём, а не сотрудником, с которым изначально была договоренность о передаче.

Выход 3 – ограничение редактирования документа.

Сотрудник при помощи программного средства ограничивает возможность редактирования документа. Таким образом секретарь не сможет произвести модификацию. Недостатком данного метода является зависимость от конкретного программного средства, поскольку не все программы могут обеспечить такую возможность.

Применение механизмов электронной цифровой подписи является очень полезным навыком, позволяющим избежать множество неприятных ситуаций, связанных с намеренной модификацией сообщений, сохранения первенства открытий и доказательства факта передачи сообщения.

Возможности MS Word в плане совместной работы

Программное обеспечение MS Word в составе MS Office позволяет облегчить возможность работы над документами группой лиц. Рассмотрим необходимые для работы функции.

Примечания

Возможность комментирования позволяет вносить примечания в определенные участки документа с указанием даты и автора примечания.

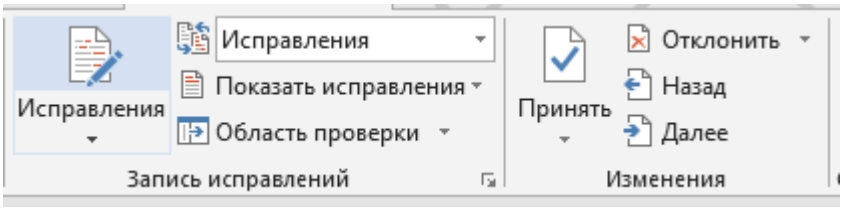
Для создания комментария, необходимо выделить комментируемый участок документа, перейти во вкладку «Рецензирование» и нажать «Создать примечание».

Для навигации между примечаниями используются кнопки «Следующее» и «Предыдущее» на вкладке. Также есть возможность показа сокрытия области примечаний.

Приложение также позволяет помечать некоторые примечания как исполненные и отвечать на примечания, таким образом создавать целые дискуссии.

Внесение исправлений

Word также позволяет вести версионность документа с отслеживанием даты и автора изменения. По умолчанию отслеживание изменений отключено для новых документов. Включение данной возможности производится на вкладке «Рецензирование». Также существует возможность принятия, отклонения изменений и просмотра исправленной версии, оригинальной версии и изменений, внесенных конкретными лицами.



Ограничение редактирования

В MS Word есть возможность блокировки определенных функций для получателей копии конкретного документа. Для создания блокировки необходимо перейти на вкладку «Рецензирование», нажать на «Ограничить редактирование», выбрать необходимые ограничения и подтвердить решение, введя пароль для защиты. Без знания пароля, получатели не смогут иметь доступ к заблокированным функциям.

Инфраструктура открытых ключей

В качестве механизма для изучения технологии сертификатов, мы рассмотрим приложение GnuPG или GPG – свободную реализацию приложения PGP (Pretty Good Privacy). Данное приложение является мощным механизмом для работы с механизмами симметричного и ассиметричного шифрования, а также механизмом для развертывания системы открытых ключей. Рассмотрим необходимые для работы функции.

Приложение GnuPG имеет реализации графических интерфейсов, тем не менее дальнейшая работа будет идти в консольном режиме.

Создание пары ключей

Для создания пары закрытый-открытый ключ необходимо произвести следующие действия:

1. Открыть эмулятор терминала.
2. Установить значение переменной PATH, добавив путь к исполняемому файлу gpg:

   set path=%path%:ПУТЬ_К_GPG/bin

3. Ввести команду создания пары ключей:

   gpg --gen-key

4. Выбрать тип создаваемого ключа RSA и RSA.
5. Оставить длину ключа и срок действия без изменений.
6. Подтвердить создание ключа указав y.
7. Ввести запрашиваемые данные и подтвердить данные.
8. При желании указать пароль к ключу.

Создание отторгаемой подписи к файлу

Для создания отторгаемой подписи (бинарная подпись в отдельном файле) ввести следующую команду:

gpg -b ПУТЬ_К_ФАЙЛУ

По окончании создания подписи, в той же папке что и файл появится файл подписи в виде ФАЙЛ.sig

Проверить подпись можно следующей командой:

gpg --verify ПУТЬ_К_ПОДПИСИ

Для файла большого по объему создание и проверка может занять длительное время.

Экспорт и импорт открытого ключа

Для того, чтобы подпись файла смог проверить получатель файла, он должен получить открытый ключ.

Экспортировать открытый ключ можно при помощи следующей команды:

gpg --export > ИМЯ_ФАЙЛА_КЛЮЧА.pub

Получатель может импортировать ключ в собственное хранилище при помощи следующей команды:

gpg --import < ИМЯ_ФАЙЛА_КЛЮЧА.pub

Задание

Для данной работы используется материал, полученный в ходе предыдущей лабораторной работы.

1. Открыть файл документации, ограничить доступ к файлу в виде записи исправлений, сохранить файл.
2. Сформировать пару ключей GPG, экспортировать открытый ключ в файл.
3. Сформировать отторгаемую подпись к файлу документации.
4. Передать файл документации, подпись и открытый ключ другому студенту, аналогичным образом получить пакет его файлов, НЕ ПЕРЕДАВАТЬ И НЕ СООБЩАТЬ СТУДЕНТУ КЛЮЧ ДЛЯ РАЗБЛОКИРОВКИ ДОКУМЕНТА.
5. Импортировать открытый ключ, проверить подпись файла.
6. Открыть файл документации, произвести не менее 10 полезных исправлений и добавить не менее 5 комментариев, сохранить файл.
7. Произвести действие аналогично п. 3 для полученного и отредактированного файла.
8. Передать отредактированный файл и получить отредактированную версию собственного файла.
9. Произвести отмену или принятие исправлений по усмотрению, принять или создать комментарии к комментариям рецензента.
10. Произвести действия 3 – 8 еще раз исключая требование к количеству исправлений и комментариев.