ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо зберігання електронних інформаційних ресурсів та їх захисту від несанкціонованого доступу.

У публікації «К вопросу о возможности использования электронной подписи в системе ЕР СФД» наведено що збільшення кількості електронних документів породжує потребу в їх страховому збереженні, що в свою чергу, ставить питання про вибір типу та виду носія для запису їх страхових копій.

Документи на електронних носіях, можуть мати силу за наявності механізму підтвердження їх справжності, цілісності та автентичності. Закладки на страхове зберігання електронних документів різних типів, з фізичним (рельєфним) нанесенням та використання електронного підпису дозволить вирішити актуальні для сучасного страхового фонду завдання.

У публікації «Несанкционированный доступ к информации» наведено загальні алгоритми проникнення у комп'ютерні системи з метою отримання необхідної інформації.

У публікації «Компьютерный терроризм «А-ля Ламмер»» розповідається про проблеми захисту інформації, наведено реальний стан справ, загальні принципи захисту інформації, використання паролів та реєстрація подій в комп'ютерних мережах. Підтверджені дані про те, що сьогодні система безпеки повинна в першу чергу гарантувати доступність і незмінність інформації під час її зберігання або передачі, а потім вже (якщо необхідно) її конфіденційність. Користувач може у будь-який час зажадати необхідний файл або ресурс, який повинен бути доступний в будь-який час (при дотриманні прав доступу), а система безпеки повинна гарантувати правильну роботу захисту. Якщо якийсь ресурс недоступний, то він марний.

У публікації «Штат Виктория, Австралия: Начато обсуждение перечня документов с указанием сроков хранения для учреждений и подразделений высшего образования и повышения квалификации» розповідається що в штаті Вікторія внесено пропозицію, зацікавленим сторонам, взяти участь в обговоренні переліку обов'язкових видів документів, що відносяться до числа архівних документів штату та не підлягають постійному зберіганню, з метою забезпечити правову основу для їх знищення після закінчення відповідних строків зберігання.

У публікації «Испания: Сертифицированная оцифровка счетов-фактур, или об опыте замещающего сканирования» розповідається, що в Іспанії «сертифікована оцифровка рахунків-фактур» - це комп'ютерний процес, що дозволяє отримати вірні електронні копії рахунків-фактур, що мають рівну юридичну силу з їх паперовими оригіналами, - і, як наслідок, чинне законодавство дозволяє знищувати паперові оригінали оцифрованих рахунків-фактур.

К ВОПРОСУ О ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В СИСТЕМЕ ЕР СФД

Источник: reprograf.ru›public.html

Авторы: Е. Е. Евсеев, П. Е. Завалишин, О. В. Чечуга, ФГУП НИИ репрографии

Единый российский страховой фонд документации (далее – ЕР СФД) является заблаговременно создаваемым, упорядоченным и надежно хранимым государственным информационным ресурсом, предназначенным для гарантированного и оперативного восстановления важнейших документов промышленных предприятий, органов исполнительной власти, учреждений науки и культуры в случае их утраты или недоступности в результате военных действий, природных и техногенных катастроф, чрезвычайных ситуаций и других форс-мажорных обстоятельств [1].

Структурно система ЕР СФД представляет собой совокупность специализированных объектов, осуществляющих изготовление, хранение и размножение страховых копий документов, организаций-поставщиков документации и органов государственной исполнительной власти, взаимодействующих по установленным государством нормам и правилам в целях осуществления информационного страхования документации.

Документы, подлежащие страховому хранению, имеют особую значимость в силу того, что на их основании принимаются ответственные решения и производится продукция, влияющая на обороноспособность и безопасность государства. Поэтому неотъемлемым свойством страховых копий таких документов должна быть не только достоверность документированной информации, но и ее юридическая сила.

Поскольку юридическая сила сообщается документу компетенцией его изготовителя и установленным порядком оформления, то особое внимание при создании страхового фонда должно уделяться установлению и соблюдению правил записи информации и реквизитов документа на носитель его страховой копии.

Исторически основным носителем для хранения страховых копий документации в системе ЕР СФД является галогенидосеребряный микрофильм. По своим физико-химическим свойствам он является исключительно надежным средством долговременного хранения информации в аналоговой человекочитаемой форме. При соблюдении определенных условий сохранения, обращения и обслуживания фонды на микрографических носителях способны гарантированно сохранять информацию сроком от 100 до 200 лет, и это доказано соответствующими испытаниями. Что же касается юридического признания, то согласно ГОСТ 13.1.101-93, в настоящее время единственными документами, закладываемыми на хранение в ЕР СФД и имеющими юридический статус

подлинника, являются микрографические носители информации, технологические процессы создания, хранения и использования которых детально регламентированы отечественными и международными стандартами [2].

В последнее время под влиянием развития новых информационных технологий происходят коренные изменения в способах создания, сохранения, передачи и использования документов. Во всех сферах жизни общества все большее распространение получают электронные документы, стремительно увеличивается электронный документооборот, традиционные документы на бумажной основе уступают место электронно-цифровым. Это относится как к организационно-распорядительным документам органов власти, так и к проектным, конструкторским, технологическим и др. документам на изделия промышленности и их составные части. Такого рода реалии привели к тому, что в 2006 году электронные документы, благодаря изменениям в государственных стандартах системы ЕСКД, официально получили одинаковый статус с традиционной (бумажной) формой документа [3].

Увеличение количества электронных документов порождает потребность в их страховом сохранении, что в свою очередь, ставит вопрос о выборе типа и вида носителя для записи их страховых копий. Если для традиционных документов на бумажной основе таким носителем является микрофильм, то для электронных документов необходим цифровой носитель, обладающий сопоставимым с микрофильмом сроком службы, повышенной устойчивостью к факторам внешней среды, надежностью в эксплуатации и низкой себестоимостью. По мнению специалистов ФГУП «НИИР», проводивших ряд исследований по указанной проблематике, таким носителями могут являться только те, при записи на которые применяется принцип физического (рельефного) нанесения информации.

Однако информационное страхование электронных документов с помощью долговременного хранения на электронных носителях, может иметь силу при наличии механизма подтверждения их подлинности, целостности и аутентичности. Поэтому другим, не менее важным вопросом использования электронных документов в системе ЕР СФД, помимо выбора носителя, является вопрос подтверждения их юридической силы в процессах создания, хранения и обеспечения пользователей. Так, согласно определению ГОСТ Р 33.0 01-2006, страховая копия документа – это специально изготовленная резервная копия документа, предназначенная для восполнения его информационного содержания и сохранения юридической силы документа в случае его утраты, повреждения или недоступности [4]. Данное определение можно распространить и на страховую копию документа на электронном носителе.

В настоящее время единственным регулятором и средством подтверждения юридической значимости электронного документа является электронная подпись, правоотношения по поводу которой закреплены в Федеральном законе Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об

электронной подписи» [5]. Последние изменения, внесенные в этот закон, существенно расширяют сферу его применения [6].

Согласно статье 5 Федерального закона № 63-ФЗ существуют следующие виды электронной подписи:

- простая электронная подпись
- усиленная неквалифицированная электронная подпись;
- усиленная квалифицированная электронная подпись.

Статья 6 того же закона гласит: «1. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

2. Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия».

При представлении документа в электронной форме его подлинность должна обеспечиваться в соответствии с ГОСТ Р 34.10-2012 и использованием квалифицированных сертификатов ключа подписи [7]. Таким образом, электронная подпись придает электронному документу юридическую силу, равную бумажному документу с подписью и печатью. Эти положения закона позволяют значительно расширить область использования электронной подписи в информационных системах различного назначения, к категории которых можно отнести и систему ЕР СФД. При этом следует учитывать, что использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается [5].

Для организации юридически значимого электронного документооборота между участниками ЕР СФД с применением электронной подписи необходима всесторонняя нормативно-правовая проработка данного вопроса и реализация комплекса соответствующих организационно-технических мероприятий.

Прежде всего, необходимо создание и аккредитация удостоверяющего центра, осуществляющего функции по созданию и выдаче сертификатов ключей проверки электронных подписей. Данный центр может быть создан как самостоятельно для решения задач обеспечения электронного документооборота в системе ЕР СФД, так и получить доверенное право на

выполнение свих функций от удостоверяющего центра более высокого уровня, что в финансовом плане является менее затратным мероприятием.

Для взаимодействия между собой и удостоверяющим центром участники системы ЕР СФД должны быть оснащены специальным программным обеспечением, а также средствами электронной подписи - шифровальными и криптографическими. При этом средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих сведения, составляющие государственную тайну, или предназначенные для использования в информационной системе, содержащей сведения, составляющие государственную тайну, подлежат подтверждению соответствия обязательным требованиям по защите сведений соответствующей степени секретности в соответствии с законодательством Российской Федерации.

Электронная подпись, если говорить о ней в контексте вопроса о процессах создания и сохранения СФД, может представлять собой защищенное хранилище (обычно в виде USB-накопителя), содержащее в себе информацию в электронной форме с данными на ответственное лицо, от имени которого производится комплектация и поставка электронной документации для закладки в ЕР СФД. Электронной цифровой подписью при передаче документации по общим и защищенным каналам связи могут заверяться все документы, отправляемые в страховой фонд, что подтверждает принадлежность поставляемой информации конкретной организации.

Учитывая высокую государственную значимость системы ЕР СФД, при возможном внедрении средств электронной подписи следует уделять повышенное внимание защите и безопасности информации. Не менее важными требованиями являются простота встраивания средств электронной подписи в информационную систему и удобство применения их конечными пользователями.

Что касается возможных проблем, которые могут возникнуть при использовании электронной подписи в системе ЕР СФД, то среди основных можно выделить недостаточную на сегодняшний день урегулированность в российском законодательстве вопросов обеспечения долгосрочного хранения электронных документов, заверенных электронной подписью. Также пока законодательно не определены технологии хранения электронных документов, не приводятся требования к обеспечению необходимого уровня безопасности для работы с электронными документами, требуемому уровню надежности системы, технологические решения по конвертации данных. Недостаточно проработаны нормативно-правовые требования для возможного извлечения и использования электронного документа без потери юридической силы через длительное время после окончания действия электронной подписи [8]. Однако данные проблемы не относятся к категории не решаемых, и со временем должны быть преодолены.

Таким образом, в связи с вышеизложенным, можно говорить о том, что подход, основанный на сочетании таких трех основных моментов, как

возможность закладки на страховое хранение электронных документов различных типов, использование электронных носителей с физическим (рельефным) нанесением информации для долговременного хранения электронных документов и применение электронной подписи позволит решить следующие актуальные для современного страхового фонда задачи:
1) закладывать в страховой фонд ранее не подлежащие закладке некоторые типы электронных документов;
2) долговременно сохранять электронные документы на специализированных электронных носителях;
3) подтверждать юридическую силу электронных документов и обеспечивать юридически значимый электронный документооборот между участниками системы ЕР СФД;
4) организовывать обеспечение пользователей документами СФД по современным телекоммуникационным каналам связи, в том числе и защищенным.

При этом существенно возрастет оперативность работы системы ЕР СФД, сократятся временные и трудовые затраты на обработку электронных документов, а также повысится качество документации, выдаваемой из страхового фонда, за счет отказа от многоступенчатых переходов информации из одной формы в другую (типа «цифра-аналог-цифра»).

Литература:

1. Постановление Правительства Российской Федерации от 26.12.1995 г. №1253-68 «Об обеспечении создания единого российского страхового фонда документации».

2. ГОСТ 13.1.101-93 «Репрография. Микрография. Микрофильм на правах подлинника. Порядок изготовления, учета, хранения и применения». – ИПК Издательство стандартов, М., 1996

3. ГОСТ 2.051-2006 Единая система конструкторской документации. Электронные документы. Общие Положения. - М.: ИПК Издательство стандартов, 2006.

4. ГОСТ Р 33.0 01-2006. ЕР СФД. Термины и определения.

5. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" // Собрание законодательства Российской Федерации, 2011, №15, ст.2036

6. Федеральный закон от 12.03.2014 N 33-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации"

7. «ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»

8. Овчинников С. А., Болдырева Е. П., Земсков М. Д. Основные проблемы сохранения цифровых записей при внедрении электронной подписи и юридически значимого электронного документооборота в России // /Вестник СГСЭУ. 2013. № 4 (48), с. 126 – 128

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ

Источник: http://www.warning.dp.ua/hackPC03.htm

Рассмотрев общие принципы защиты информации в компьютерных системах, можно перейти к попыткам ее похищения. Рассмотрим общие алгоритмы.

Используемые сокращения:

ЗИ - защита информации;

НСД - несанкционированный доступ;

ПК - персональный компьютер;

КС - компьютерная система;

ОС - операционная система;

BIOS - Базовая Система Ввода-Вывода (англ.: Basic Input Output System).

Аппаратные средства взлома

1. Похищение информации с КС

Подкуп должностных лиц, имеющих доступ к атакуемой КС, и похищение требуемой информации. Я думаю, комментарии здесь излишни. Будьте внимательны, чтобы люди, которых вы подкупаете, не оказались сотрудниками службы безопасности атакуемого учреждения…

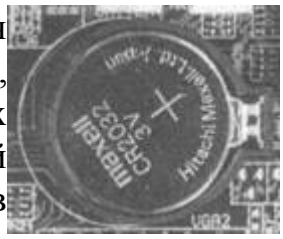
2. Обход электронно-механических ключей для запуска персонального компьютера

По данному вопросу можно было бы писать очень много, т.к. стандартных систем и ключей защиты на нашей обширной родине в принципе не выпускается, и делают их либо электротехники-любители, либо узкоспециализированные фирмы по конкретному заказу отдельных учреждений. А поэтому системы и принципы функционирования могут варьироваться от обычного замка на корпусе ПК в месте кнопки включения питания, до специальных электронных ключей, включающихся в цепь блока питания ПК и блокирующих возможность включения питания без соответствующего электронного или электронно-механического ключа. Тут как говорится без топора не обойтись, причем в прямом смысле слова… Проще физически взломать защиту и бесследно исчезнуть с места, чем ломать себе голову как более эффективно обойти защиту.

Программные средства взлома

3. Сброс CMOS и паролей на начальную загрузку ПК / изменение установок BIOS

Теория. Все настройки и в частности пароли BIOS (являются неотъемлемой частью настроек) хранятся в памяти CMOS RTC RAM[a], подпитываемой аккумулятором, который расположен на материнской плате ПК. Стереть настройки можно двумя способами – аппаратным и программным.



Цель. Технология сброса данных CMOS используется для обхода User Password и/или Supervisor Password, установленных в BIOS, и/или внесения требуемых временных изменений в настройки BIOS. Т.е. конечной целью является получение доступа к установленной ОС в ПК.

Методика. Чтобы аппаратно стереть CMOS проделайте следующее:

1) Отключите компьютер если это необходимо.
2) Выберите удобный вам способ сброса CMOS:

Мягкий. Быстрый и стандартный. Найдите на материнской плате 3-х контактный джампер (перемычку на 2 положения) с надписью **Clear CMOS§ / Hold CMOS** и замкните на несколько секунд джампер в противоположное положение (**Clear CMOS**). Затем верните перемычку назад в исходное положение (**Hold CMOS**). Если вы не уверены – лучше используйте жесткий метод *(см. ниже)*.

Жесткий. Более медленный, но более надежный по сравнению с предыдущим. Найдите на материнской плате круглый аккумулятор. Выньте его из разъема ~ на 15 секунд и вложите обратно.

3) Включите компьютер.

Данный метод будет работать только в случае отсутствия пломб на системном блоке ПК, хотя если вы производите единичное вторжение и выбрали именно этот способ – *вскрытие пломб неизбежно*.

Помните! Опытные хакеры не оставляют следов!

Более приемлимым, однако менее работоспособным, является программный способ очистки CMOS. В этом способе используются специальные *утилиты очистки данных CMOS* (что-то вроде KillCmos, RemPass и т.п.). Найти их можно в Интернете почти на любом уважаемом хаккерском сайте.

Внимание! При очистке данных CMOS вы сбросите установленные пароли BIOS и другие настройки BIOS, что сразу же укажет на несанкционированный доступ к ПК (особенно если в BIOS установлен User Password).

Чтобы обойти это при возможности загрузки хотя бы в DOS, можно воспользоваться специальными *утилитами для сохранения и восстановления настроек CMOS* – напр. англ.: Flash Memory Writer для BIOS фирмы Award. Их можно скачать в Internet на сайтах производителей материнских плат под конкретную версию BIOS. Если версия и тип BIOS атакуемого ПК неизвестен – лучше запастись утилитами под максимально более обширный диапазон версий и типов BIOS (наиболее распространенные Award, AMI).

План любой атаки будет иметь 2 возможные реализации и выглядеть примерно так:

- Есть возможность загрузиться в любую ОС.
- Загрузка в доступную ОС и сохранение настроек CMOS с помощью указанной утилиты *(см. выше)*.
- Сброс данных CMOS программным или аппаратным способом.
- Установка требуемых временных настроек CMOS (например, разрешение загрузки с дискеты).
- Непосредственно сама атака: похищение требуемой информации, установка клавиатурных шпионов, троянов и т.п.
- Загрузка сохраненных настроек CMOS с помощью все той же вышеупомянутой утилиты.
- Нет возможности загрузиться в любую ОС.
- Сброс данных CMOS аппаратным способом.
- Установка требуемых временных настроек CMOS.
- Непосредственно сама атака: похищение требуемой информации, установка клавиатурных шпионов, троянов и т.п.
- Загрузка сохраненных настроек CMOS с помощью все той же вышеупомянутой утилиты.

Примечание. В случае если в системе был установлен пароль(и) на BIOS, был осуществлен сброс CMOS, а восстановление настроек CMOS по каким-либо причинам не возможно, для запутывания противника можно установить свой пароль на BIOS – это даст выигрыш во времени и в определенной степени смутит неопытного владельца.

4. Разрешение загрузки ПК с дискеты

Теория. Если загрузка с дискеты запрещена, ее можно разрешить, что даст доступ к жесткому диску компьютера и данных на нем. Причем даже если это NTFS-раздел, данные можно как минимум похитить. Подробнее *см. ниже*.

Цель. Досуп к ОС, а также информации на жестком диске.

Методика.

1) Если нет доступа к BIOS – сбросьте CMOS *(см. Пункт 3)*.
2) Войдите в режим настройки BIOS.
3) Затем в секции **Advanced BIOS Features [Boot]** пункт **Legasy Floppy** нужно установить на первую позицию в **Boot Sequence** чтобы попытка загрузки с гибкого диска была первой.
4) Сохраните внесенные изменения BIOS.

5. Похищение пароля пользователя с помощью клавиатурного шпиона

Теория. Существует множество клавиатурных шпионов, однако у всех у них есть один существенный недостаток – в ОС семейства Windows NT похищение пароля не возможно по следующей причине – автоматический запуск программ происходит намного позже после аутентификации. Единственная возможность – надежда на введение паролей в прикладные программы во время рабочего сеанса, либо же подмена системного драйвера

клавиатуры. При выборе "шпиона" руководствуйтесь следующими принципами:

- "Шпионы" различаются конкретной системной реализацией, т.е. на какую ОС рассчитан данный шпион (будьте внимательны – некоторые шпионы не работают под ОС семейства Windows NT);
- Не используйте популярных "шпионов", т.к. скорее всего они засвечены в среде популярных антивирусов. Т.н. известный и очень популярный шпион HookDump предоставляет обширные опции, однако его существенным недостатком является обнаружение оного большинством антивирусных программ (DrWeb, Kaspersky Antivirus и т.п.).
- Возможность отправки отчета по электронной почте не заметно от владельца компьютера.

Цель. Похищение пароля пользователя и доступ к информации под видом легального пользователя.

Методика.

Установите в компьютерной системе клавиатурного шпиона. Метод автор оставляет за вами.

6. Стандартные пароли в операционных системах

Теория. © *Автор метода неизвестен*. Как говорилось ранее, в некоторых случаях возможен подбор пароля, для входа в систему. До недавнего времени, пользователи выбирали пароли которые легко запомнить, или даже оставляли те, которые стоят в системе по умолчанию при инсталляции. Также, очень часто пользователи используют в качестве паролей, свое имя, фамилию, имя своего бюджета, или вообще его не ставят.

Методика. Если у вас не хватает фантазии, вы можете поэкспериментировать с этим списком:

admin, ann, anon, anonymous/anonymous, backup, batch, bin, checkfsys, daemon, demo, diag, field, ftp, games, guest/guest, guest/anonymous, help, install, listen, lp, lpadmin, maint, makefsys, mountfsys, network, news, nobody, nuucp, nuucpa, operator, powerdown, printer, pub, public, reboot, rje, rlogin, root, sa, setup, shutdown, startup, sync, sys/sys, sysadm, sysadmin, sysbin/sysbin, sysbin/bin, sysman, system, tech, test, trouble, tty, umountfsys, user/user, user1/user1, uucp, uucpa, visitor.

Примечание. Вы уже поменяли свой пароль?

7. Похищение информации / паролей с помощью трояна

Теория. Для похищения различной информации с удаленного компьютера, к которому вы не имеете доступа, можно использовать всяческие сетевые вирусы-троянцы, которые можно замаскировать под ускоритель DirectX или еще чего ни будь в этом роде. При этом желательно пользоваться самописными троянцами и проверять их популярными антивирусами перед забросом во вражеский лагерь. Или, например, пересоздать инсталляционный пакет того же DirectX (например, DirectX 10

beta – актуально на 08.10.03) с сохранением всех опций и файлов, но добавив в него клавиатурного шпиона с файлом заранее установленных настроек. Причем нужно настроить инсталляционный пакет так, чтобы шпион был запущен сразу же после инсталляции продукта или в процессе оной. Некоторые шпионы поддерживают опцию "тихой" пересылки LOG-файла по электронной почте, т.е. скрытую от глаз пользователя. Опытный администратор может элементарно отследить это, поэтому параллельно со шпионом можно самому написать программу, которая в определенное установленное время сотрет и шпиона и себя с атакуемого компьютера (это может быть дополнительная функция в самом шпионе). **З.Ы.:** О том как вы будете впаривать ваш "типа" самый последний beta DirectX владельцам атакуемого ПК – думайте сами!

Исходя из личного опыта могу дать совет прикладного характера по примерным местам похищения паролей. Обычно в корпоративных сетях услуги Интернета предоставляются через т.н. прокси-сервер, т.е. это может быть отдельный компьютер (специально выделенный для этих целей), а может быть и главный сервер. С программной точки зрения прокси-сервер выгоден тем, что он является шлюзом между Интернетом и общей сетью. С его помощью можно установить привилегии пользователей, напр. запретить кому-нибудь из пользователей качать из Интернета музыку и т.п. Однако для этого должна использоваться технология Авторизации Пользователей. В последнем случае неграмотный пользователь при очередном запросе логина и пароля может устать от его ввода и установить галочку "Запомнить пароль"… С точки зрения человека, который не имеет доступа к его компьютеру это ничего не даст. Однако если использовать троянца, можно украсть эти логин и пароль, ведь они хранятся в КЭШе. Таким образом, вы сможете получить доступ к системе. Конечную реализацию я оставляю на продвинутых хакеров-программистов.

Еще одним уязвимым местом подобного характера являются системы обмена сообщениями в реальном времени, например, одна из наиболее популярных – ICQ. Она также запрашивает в настройках параметры прокси-сервера в числе которых есть пункт авторизации, т.е. те самые пресловутые логин и пароль, которые нам так нужны. Опять же реализация за вами. Данный метод автором лично не проверялся, однако с теоретической точки зрения он может подтвердиться в 10% случаев (зависит от установок авторизации на прокси-сервере), что тоже хорошо.

8. Дешифрование защищенной информации / восстановление паролей

Теория. Сие знание здесь явно не будет раскрыто, ибо для дешифрования информации нужно быть хоть чуть-чуть крипто-аналитиком, знать основные принципы шифрования, наиболее распространенные крипто-алгоритмы *(см. "Криптографическая ЗИ" PAGEREF _Ref49343587 \p \h на стр. 277)* и владеть несколькими языками программирования. Т.е. по сути, быть инженером-программистом. Это отдельная тема разговора в отдельной книге.

Однако не расстраивайтесь. Если данные зашифрованы в файле стандартного формата, не стоит тратить время на дешифрование данных, проще подобрать пароль, что и реализовано в множестве программ. Как известно при шифровании данных в файле хранится не сам пароль, а его хеш-сумма. Зная положение этой хеш-суммы, можно осуществить атаку по подбору оригинального пароля. Обычно используется либо метод полного перебора – при этом перебираются все возможные комбинации паролей, а на каждом шаге получения комбинации из нее формируется ее хеш-сумма, которая и сравнивается с хеш-суммой в файле. Другим вариантом является атака по словарю – в этом случае всё аналогично методу перебора, только вместо перебора комбинаций используется отдельный файл, содержащий наиболее употребимые пароли, и из них уже формируются сравниваемые хеш-суммы.

Цель. Взлом защищенных данных.

Методика.

Существуют множество программ для взлома наиболее популярных и распространенных форматов файлов.

- **PWLInside 1.22**
- Поддерживаемые ОС: Win 9x/Me/2000/XP.
- Технические характеристики:

- Подбор забытых паролей к *.PWL-файлам операционных систем Windows'3.11/95/OSR2/98/ME методом полного перебора.

- Подбор забытых паролей к *.PWL-файлам операционных систем Windows'OSR2/98/ME по внешнему словарю.

- Получение списка всех ресурсов с паролями к ним, расположенных в исходном *.PWL-файле при нахождении правильного пароля, либо при использовании ключа /P с верным паролем.

- Расшифровка паролей к ресурсам из реестра от всех вышеперечисленных операционных систем, сохраненного в текстовом виде.

- Преимущества: Перебор паролей в 2-3 раза быстрее, чем у аналогичных программ.
- Официальный сайт: http://www.insidepro.com/rus/pwlinside.shtml/.

Примечание. Так называемые PWL-файлы – это файлы с именами пользователей компьютера и с расширениями *.PWL (к примеру, Master.PWL, Sales.PWL и пр.), которые находятся в системной директории Windows. Это файлы, в которых хранятся различные аккаунты конкретного пользователя, т.е. в нем находятся пароли к расшаренным ресурсам сети (к которым подключался данный юзер, а не к ресурсам текущего компьютера), пароли на вход в NetWare/NT-сервера, пароли на Dial-Up-соединения и пр. Естественно, эти данные зашифрованы определенными алгоритмами и для их дешифрования необходимо знать пароль пользователя – а это фактически пароль на вход в Windows. А так как людям свойственно забывать свои пароли, то подбор пароля, во-первых, позволяет его "вспомнить", а, во-вторых, позволяет просмотреть список аккаунтов этого пользователя, которые Windows сохраняет в этом PWL-файле.

- **SAMInside 2.1**
- Поддерживаемые ОС: Win 9x/Me/2000/XP.
- Технические характеристики:
- Получение информации о пользователях из SAM-файлов Windows'NT/2000/XP.
- Подбор паролей пользователей из SAM-файлов операционной системы Windows'NT.
- Подбор паролей пользователей из SAM-файлов операционных систем Windows'2000/XP, зашифрованных системным ключом Syskey!
- Преимущества: Перебор паролей в несколько раз быстрее, чем у аналогичных программ.
- Недостатки: Программа платная, в демо-версии нельзя использовать другой алфавит для перебора (цифры, национальные символы и пр.), кроме заглавных латинских букв, а также нельзя производить перебор паролей по словарю.
- Официальный сайт: http://www.insidepro.com/rus/saminside.shtml/.

- **PacketCatch 1.0**
- Поддерживаемые ОС: Win 9x/Me/2000/XP.
- Технические характеристики:
- Перехват SMB-пакетов операций входа в сеть пользователей и отображение следующей полученной информации: имя пользователя; IP адрес, с которого произведен вход; IP адрес сервера, на который произведен вход; Challenge сессии; зашифрованный LMHash; зашифрованный NTHash.
- Установка маски подсети, в которой производить перехват.
- Сохранение результатов в формате, который понимают другие программы для восстановления паролей к хэшам пользователей.
- Официальный сайт: http://www.insidepro.com/rus/packetcatch.shtml/.

9. Восстановление удаленных данных

Теория. *См. "Невосстановимое удаление данных" PAGEREF _Ref52634043 \p \h на стр. 283*.

Цель. Восстановить удаленные данные с носителей информации.

Методика. Программное обеспечение:

- **Active@ UNERASER**
- Поддерживаемые ОС: Win 9x/Me/NT/2000/XP.
- Технические характеристики:
- Восстановление удаленных файлов и папок с разделов на жестком диске, а также данных после форматирования разделов или вирусных атак;
- Возможность запуска с дискеты;
- Поддерживаемые устройства: IDE, ATA и SCSI жесткие диски, дискеты;
- Съемные устройства: CompactFlash, SmartMedia, Secure Digital / MultiMediaCard, и т.п.;

- Диски большого размера (больше 8Гб), длинные имена файлов с локализацией языка;
- Восстановление сжатых и фрагментированых файлов на NTFS разделах;
- Создание "образа" раздела(ов);
- Архивация/восстановление загрузочной записи (MBR), таблицы размещения файлов и загрузочных секторов разделов жесткого диска.
- Поддержка LBA-режима для доступа к дискам большого размера;
- Чтение и копирование файлов с NTFS на FAT разделы.
- Поддерживаемые файловые системы.
- FAT12, FAT16, FAT32, NTFS, NTFS5;
- Недостатки: Программа платная, в демо-версии стоит ограничение на максимальный размер восстанавливаемого файла.
- Официальный сайт: http://www.uneraser.com/.

- **GetDataBack**
- Поддерживаемые ОС: Win 9x/Me/NT/2000/XP.
- Технические характеристики:
- Восстановление удаленных файлов и папок с разделов на жестком диске даже в случае повреждения таблицы размещения файлов, загрузочной записи, а также данных после форматирования разделов, вирусных атак или потери питания, переразбивки диска с помощью утилиты fdisk;
- Возможность восстановления данных с сетевого диска (необходима дополнительная утилита);
- Длинные имена файлов;
- Поддерживаемые устройства: жесткие диски, дискеты;
- Съемные устройства: Zip/Jaz диски, CompactFlash, SmartMedia, Secure Digital карты, USB Flash;
- Поддерживаемые файловые системы. Существует в двух версиях для файловых систем:
- FAT;
- NTFS.
- Недостатки: Программа платная (для FAT систем – $69, для NTFS – $79).
- Официальный сайт: http://www.runtime.org/gdb.htm.

10. Доступ к данным на NTFS разделах

Теория. FAT файловая система была переходным звеном от ОС DOS к Windows 9x/ME, а посему ни о какой защите личной информации не может быть и речи. NTFS сменила FAT с выходом ОС нового поколения – семейства Windows NT. В NTFS файловой системе реализована аутентификация доступа к данным. Доступ к NTFS разделам из ранних версий Windows запрещен в силу политики защиты информации, а также чисто с технической позиции – принципиально разная структура файловых систем.

Цель. Получить доступ к данным на NTFS разделе.

Методика. Программное обеспечение:

- **NTFS for Windows**
- Поддерживаемые ОС: Win 9x.
- Технические характеристики:
- Чтение данных с NTFS разделов жесткого диска;
- Недостатки: Программа платная.
- Официальный сайт: http://www.sysinternals.com/ntw2k/freeware/ntfswin98.shtml.

- **NTFS for DOS**
- Поддерживаемые ОС: DOS/Windows.
- Технические характеристики:
- Чтение и выполнение файлов с NTFS разделов жесткого диска в обход NTFS защиты;
- Недостатки: Программа платная.
- Официальный сайт: http://www.sysinternals.com/ntw2k/freeware/ntfsdos.shtml.

[a] RTC RAM (англ.: Real Time Clock Random Access Memory) – оперативная память часов реального времени.

§ Возможный вариант – англ.: Reset CMOS.

КОМПЬЮТЕРНЫЙ ТЕРРОРИЗМ «А-ЛЯ ЛАММЕР»

Источник: http://www.warning.dp.ua/hackPC04.htm

"Мы существуем независимо от национальности, цвета кожи и религиозного уклона. Мы повсюду – в школе, в клубе, в вашем сознании… Вы развязываете войны, лжёте и творите беспредел!!! Я преступник, но моё преступление заключается только в любопытсве – я ХАКЕР!!! Вы можете остановить меня, но нас всех остановить невозможно!!!"

Манифест Хакера

Используемые сокращения:

ЗИ - защита информации;

НСД - несанкционированный доступ;

ПК - персональный компьютер;

КС - компьютерная система;

ОС - операционная система;

BIOS - Базовая Система Ввода-Вывода (англ.: Basic Input Output System).

Мифы компьютерной безопасности

Автор: Валерий Коржов.

Проблема защиты информации не нова. Она появилась вместе с компьютерами. Естественно, что стремительное совершенствование компьютерных технологий отразилось и на принципах построения защиты информации. Задачи изменились, а мнения остались прежние – так рождаются мифы. Вот несколько мифов компьютерной безопасности.

Миф первый

"Защита информации и криптография – близнецы-братья".

Этот миф, видимо, связан с тем, что с самого начала своего развития системы информационной безопасности разрабатывались для военных ведомств. Разглашение такой информации могло привести к огромным жертвам, в том числе и человеческим. Поэтому конфиденциальности (т.е. неразглашению информации) в первых системах безопасности уделялось особое внимание. Очевидно, что надежно защитить сообщения и данные от подглядывания и перехвата может только полное их шифрование. Видимо из-за этого начальный этап развития компьютерной безопасности прочно связан с криптошифрами.

Однако сегодня информация имеет уже не столь "убойную" силу, и задача сохранения ее в секрете потеряла былую актуальность. Сейчас главные условия безопасности информации – ее доступность и целостность. Другими словами, пользователь может в любое время затребовать необходимый ему сервис, а система безопасности должна гарантировать его правильную работу. Любой файл или ресурс системы должен быть доступен в любое время (при соблюдении прав доступа). Если какой-то ресурс недоступен, то он бесполезен. Другая задача защиты – обеспечить неизменность информации во время ее хранения или передачи. Это так называемое условие целостности.

Таким образом, конфиденциальность информации, обеспечиваемая криптографией, не является главным требованием при проектировании защитных систем. Выполнение процедур криптокодирования и декодирования может замедлить передачу данных и уменьшить их доступность, так как пользователь будет слишком долго ждать свои "надежно защищенные" данные, а это недопустимо в некоторых современных компьютерных системах. Поэтому система безопасности должна в первую очередь гарантировать доступность и целостность информации, а затем уже (если необходимо) ее конфиденциальность. Принцип современной защиты информации можно выразить так – поиск оптимального соотношения между доступностью и безопасностью.

Миф второй

"Во всем виноваты хакеры".

Этот миф поддерживают средства массовой информации, которые со всеми ужасающими подробностями описывают "взломы банковских сеток". Однако редко упоминается о том, что хакеры чаще всего используют

некомпетентность и халатность обслуживающего персонала. Хакер – диагност. Именно некомпетентность пользователей можно считать главной угрозой безопасности. Также серьезную угрозу представляют служащие, которые чем-либо недовольны, например, заработной платой.

Одна из проблем подобного рода – так называемые слабые пароли. Пользователи для лучшего запоминания выбирают легко угадываемые пароли. Причем проконтролировать сложность пароля невозможно. Другая проблема – пренебрежение требованиями безопасности. Например, опасно использовать непроверенное программное обеспечение. Обычно пользователь сам "приглашает" в систему вирусы и "троянских коней". Кроме того много неприятностей может принести неправильно набранная команда. Так, при программировании аппарата ФОБОС-1 ему с Земли была передана неправильная команда. В результате связь с ним была потеряна.

Таким образом, лучшая защита от нападения – не допускать его. Обучение пользователей правилам сетевой безопасности может предотвратить нападения. Другими словами, защита информации включает в себя кроме технических мер еще и обучение или правильный подбор обслуживающего персонала.

Миф третий

"Абсолютная защита".

Абсолютной защиты быть не может. Распространено такое мнение – "установил защиту и можно ни о чем не беспокоиться". Полностью защищенный компьютер – это тот, который стоит под замком в бронированной комнате в сейфе, не подключен ни к какой сети (даже электрической) и выключен. Такой компьютер имеет абсолютную защиту, однако, использовать его нельзя. В этом примере не выполняется требование доступности информации. "Абсолютности" защиты мешает не только необходимость пользоваться защищаемыми данными, но и усложнение защищаемых систем. Использование постоянных, не развивающихся механизмов защиты опасно, и для этого есть несколько причин.

Одна из них – развитие вашей собственной сети. Ведь защитные свойства электронных систем безопасности во многом зависят от конфигурации сети и используемых в ней программ. Даже если не менять топологию сети, то все равно придется когда-нибудь использовать новые версии ранее установленных продуктов. Однако может случиться так, что новые возможности этого продукта пробьют брешь в защите.

Кроме того, нельзя забывать о развитии и совершенствовании средств нападения. Техника так быстро меняется, что трудно определить, какое новое устройство или программное обеспечение, используемое для нападения, может обмануть вашу защиту. Например, криптосистема DES, являющаяся стандартом шифрования в США с 1977 г., сегодня может быть раскрыта методом "грубой силы" – прямым перебором.

Компьютерная защита – это постоянная борьба с глупостью пользователей и интеллектом хакеров.

В заключение хочется сказать о том, что защита информации не ограничивается техническими методами. Проблема значительно шире. Основной недостаток защиты – люди, и поэтому надежность системы безопасности зависит в основном от отношения к ней служащих компании. Помимо этого, защита должна постоянно совершенствоваться вместе с развитием компьютерной сети. Не стоит забывать, что мешает работе не система безопасности, а ее отсутствие.

Что же такое информация?

Информация – это первичное понятие этого мира и строго определена быть не может. Объективное определение: информация приносит знания о мире, которых до ее получения не было. Она передается в пространстве и времени с помощью материальных носителей (знаков, символов). Для передачи информации и ее хранения может быть использовано любое физическое явление или объект. Она может быть полезной, нейтральной и вредной для конечного получателя. С течением времени информация может носить убывающий характер (повседневная информация в обществе – напр. прогноз погоды на завтра) или волнообразный характер (научная информация).

Реальное положение дел сегодня

Ушедшее столетие принесло человечеству одновременно огромную радость и огорчение – компьютер. Для одних – это домашний кинотеатр, для других – домашняя студия звукозаписи, для третьих – средство управления технологическим процессом сборки автомобилей или теми же банковскими переводами… При этом круг лиц, имеющих доступ к компьютерным системам, постоянно растет, а их моральный облик падает. Поэтому наиболее актуальный вопрос всех времен – это вопрос защиты информации. Ему уделяется 30-35% времени и финансирования во всех крупных компаниях, занимающихся разработкой программного обеспечения. Различается две группы лиц:

- Владельцы информации, нуждающиеся в защите своей информации;
- Похитители информации, пытающиеся осуществить Несанкционированный Доступ (НСД) в систему и похитить оную информацию.

В последующих главах мы не будем вдаваться в подробности строения и функционирования компьютерных систем (для этого есть множество соответствующей справочной литературы), а проведем сравнительный анализ наиболее реальных действий представителей обоих групп, направленных для достижения их конечных целей. Однако перед этим окунемся немного в теорию ЗИ.

Проблемы защиты информации

У владельцев информации в связи с их конечной целью защиты информации имеются следующие проблемы:

- Обеспечение целостности информации (защита от искажения и уничтожения при хранении/передаче);
- Защита от НСД;

- Защита пользователей от компроментации;
- Исключение отказов от принятых обязательств.

Центральной является проблема защиты от несанкционированного доступа, т.к. именно через него реализуются попытки искажения, уничтожения или злонамеренного использования информации.

Виды и цели вторжений

Злоумышленники, пытающиеся осуществить НСД, делятся на 2 группы:

- Нелегальные;
- Легальные пользователи, имеющие законный доступ, но пытающиеся превысить свои полномочия.

Попытки НСД называются вторжениями, которые в свою очередь подразделяются на:

- Пассивные вторжения. Их крайне трудно обнаружить. Имеют следующие цели:
- Определение объемов, интенсивности, направления передачи и содержания передаваемой информации;
- Получение сведений о паролях, идентификаторах, именах абонентов и т.п.;
- Получение информации о структуре системы и средствах ее защиты, уровнях прав доступа и механизмах их изменения.
- Активные вторжения. Имеют следующие цели:
- Искажение и уничтожение информации;
- Распространение дезинформации и компроментация пользователей;
- Получение информации о паролях, ключах, идентификаторах, системе защиты и правах доступа;
- Перехват управления системой.

Общие принципы ЗИ в КС

Чтобы лучше понять методы защиты информации, а параллельно и набросать примерные способы ее похищения, рассмотрим некую абстрактную систему ЗИ в КС. Мы не будем привязываться к конкретной архитектуре системы, ведь будь то ОС семейства Microsoft Windows NT, или Unix-подобная ОС – основные принципы везде одинаковы, различия заключаются лишь в конечной реализации алгоритма.

Модель ЗИ

Взглянем на известную модифицированную *модель Белла и Ла-Падула*. В нее входят:

- Субъекты – пользователи;
- Объекты – защищаемые ресурсы (диски, каталоги и т.п.);
- Диспетчер Доступа (ДД);
- Матрица Прав Доступа (МПД);
- Служба Аутентификации (СА);
- Матрица Паролей (МП).

В любой компьютерной системе существует понятие идентификации – присвоения объекту или субъекту уникального имени-идентификатора, по которому его можно отличить от других объектов или субъектов:

- Для объектов идентификатором является путь (напр. имя диска, путь к каталогу, путь к файлу). Путь зачастую задается субъектами (напр. имена каталогов и файлов).

- Для субъектов идентификатором является т.н. логин (имя субъекта). Список субъектов контролирует системный администратор[a], он же назначает права доступа субъектов системы к ее объектам (модифицирует МПД). В некоторых реализациях систем ЗИ субъект (обычный пользователь) в зависимости от принадлежности к той или иной группе пользователей (напр. группа администраторов в ОС семейства Microsoft Windows NT) может сам создавать новых субъектов и модифицировать МПД. В других – субъект таких действий выполнять не может.

Как правило, вначале рабочего сеанса с системой происходит аутентификация (установление подлинности) – проверка того, является ли субъект действительно тем, за кого себя выдает. Для аутентификации широко используются:

- Пароли – система запрашивает *логин* и *пароль* субъекта, которые передаются Службе Аутентификации. СА в свою очередь сверяет введенные данные с данными в Матрице Паролей. Если субъект с введенным логином существует и введенный пароль совпадает с паролем в МП – выполняется вход в систему, иначе – отклоняется *(подробнее см. "Пароли и параметры* их стойкости*" PAGEREF _Ref49218191 \p \h ниже)*;

- Биометрические системы контроля – анализ клавиатурного почерка, считывание отпечатков пальцев, верификация голоса, сканирование сетчатки глаза, считывание геометрии рук, распознавание подписи и т.п.;

- Электронные и физические ключи, магнитные карты и т.п.

Основное действие, происходящее при любом обращении субъекта к объекту: определение полномочий – установка в какой мере проверяемому субъекту дано право обращаться к защищаемому объекту. В общем случае это выглядит так: некий субъект (пользователь) обращается к объекту (напр. хочет просмотреть содержимое католога). При обращении, управление передается Диспетчеру Доступа, а также информация о субъекте, объекте и затребованном действии (чтение, запись, просмотр и т.п.). ДД обращается в МПД и определяет права доступа субъекта по отношению к объекту. Если права на затребованное действие имеются – действие выполняется, иначе – оное отклоняется.

Т.е. как таковая работа с абстрактной КС может выглядеть так:

1. Идентификация пользователя. Происходит в первый раз работы с системой.
2. Аутентификация. Происходит в начале каждого рабочего сеанса с системой.
3. Цикл нижеприведенных действий выполняется постоянно при любом обращении к любому объекту системы в течении рабочего сеанса:

а. Определение полномочий.

б. Регистрация результата в журнале событий. *(см. "Регистрация событий в системе" PAGEREF _Ref49220081 \p \h на стр. 277)*.

4. Выход из системы. Происходит в конце каждого рабочего сеанса с системой.

Пароли и параметры их стойкости

Пароль – строка символов, введенных с клавиатуры. Самый простой, удобный и дешевый метод аутентификации. Однако в этом случае возникает проблема возможного угадывания или кражи паролей.

Эффективность пароля принято оценивать т.н. ожидаемым безопасным временем раскрытия его методом перебора§. Это время рассчитывают по формуле:

Тб = ½ N * t = ½ AS * E/R,

где N – число возможных паролей, t – время ввода одного набора, A – число символов алфавита конечного пароля, S – длина пароля, E – количество символов, требуемое для ввода пароля с учетом служебных клавиш Enter…Shift, R – скорость ввода символов.

Т.о. можна вывести основные параметры стойкости паролей:

- Длина пароля. Чем длиннее пароль – тем сложнее и дольше его взломать. В этом случае возрастает количество возможных комбинаций пароля. Длина пароля должна быть не менее 16 символов для относительно надежной защиты от метода перебора.

- Количество символов в алфавите. Аналогичный эффект вышеприведенному.

Основные меры предосторожности при работе с паролем

- Не следует использовать в качестве пароля:

- Собственные имена, имена друзей, любимых людей, клички, даты рождения, и т.п. данные, легко доступные похитителям информации;

- Профессиональные термины, жаргон и т.п.;

- Повторяющиеся символы;

- Реальные слова и их комбинации – для получения легко запоминаемых устойчивых паролей можно пользоваться соответствующими генераторами, которые генерируют пароли, состоящие из цифр и букв различного регистра.

- Следует учитывать используемый алфавит (количество символов в нем).

- Пароль необходимо часто менять, в зависимости от уровня защиты системы. Классически – каждый месяц.

- Еще одна ошибка типичного пользователя – ввод пароля в одной раскладке (напр. русской) с включенной другой раскладкой (напр. английской). Подобные ситуации приводят к хищению пароля более менее наблюдательным человеком, который находится рядом с компьютером в момент ввода пароля. Не считайте себя умнее других.

Регистрация событий в системе

Еще один важный момент работы с системой. Про него забывают многие т.н. хакеры, когда пытаются взломать различные системы, на чем собственно и попадаются. Как я уже говорил, любое обращение пользователя к ресурсу сопровождается определением полномочий. Однако сразу же после этого выполняется т.н. регистрация события в системе. Результат определения полномочий записывается в Журнал безопасности. Он содержит записи о таких событиях, как успешные и безуспешные попытки доступа в систему, а также о событиях, относящихся к использованию ресурсов, например о создании, открытии и удалении файлов и других объектов.

Решение о событиях, сведения о которых заносятся в журнал безопасности, принимает системный администратор. Например, после разрешения аудита входа в систему сведения обо всех попытках входа заносятся в журнал безопасности.

С журналом безопасности тесно связаны два понятия:

- Аудит успехов – событие, соответствующее успешно завершенному действию, связанному с поддержкой безопасности системы. Например, в случае успешного входа пользователя в систему, в журнал заносится событие с типом *Аудит успехов*.
- Аудит отказов – событие, соответствующее неудачно завершенному действию, связанному с поддержкой безопасности системы. Например, в случае неудачной попытки доступа пользователя к сетевому диску в журнал заносится событие типа *Аудит отказов*.

Попросту говоря каждый ваш шаг и каждое ваше действие в КС фиксируется в журнале. И опытный администратор с легкостью вычислит попытки проникновения в систему, если оный журнал не очистить. Последнее действие (очистка журнала) внесет нотки сомнения в душу администратора и возможно он подумает о системном сбое (хотя это маловероятно), что даст вам некоторое время ретироваться. Вероятность того, что аудит в системе отключен в серьезных организациях практически сводится к нулю *(подробнее см. Глава 9.3 "Несанкционированный доступ к информации" PAGEREF _Ref49331336 \p \h на стр. 293)*. С учетом всего вышеприведенного, хотелось бы сказать следующее: *"Граждане, мойте пол после себя, если ходите в грязных калошах по чужому дому в отсутствие хозяев!"*

Криптографическая ЗИ

Кроме методов защиты информации в КС, рассмотренных выше и применимых только внутри системы, пользователями (а зачастую и самой КС) могут использоваться дополнительные средства ЗИ – шифрование данных. Ведь при транспортировке данных вне КС, они могут быть похищены, изменены (например, при передаче по сети) или случайно скопированы заинтересовавшимся человеком. Ущерб в этом случае может быть довольно серьезен. Или возьмем тот же банковский перевод денежных средств. Там все передаваемые данные обязательно шифруются!

Криптография – наука о способах преобразования данных, позволяющих сделать их бесполезными для противника. Способы (алгоритмы) такого преобразования называются шифрами. Любая попытка перехватчика расшифровать шифр текста или зашифровать свой собственный открытый текст для получения правдоподобного шифр-текста при отсутствии подлинного ключа называют криптоаналитической атакой. Если это не возможно, то систему называют криптостойкой. Криптостойкая система оценивается временем раскрытия шифра. Наука о способах и методах раскрытия шифров называется криптоанализом.

Криптосистемы и принцип шифрования

По количеству ключей шифрования различают:

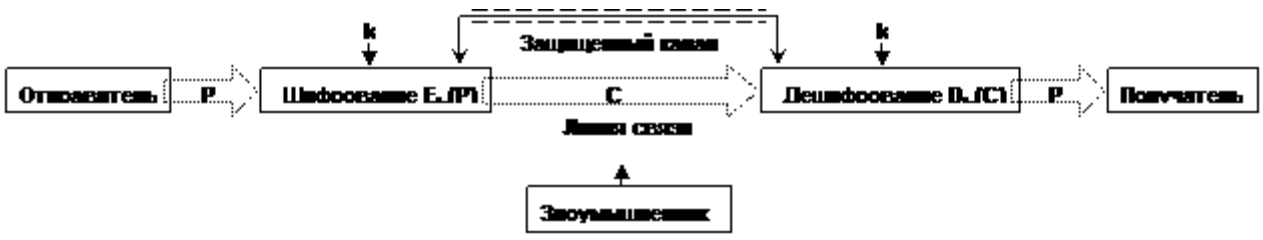
- Симметричные криптосистемы (с 1-м ключем);
- Асиметричные криптосистемы (с 2-мя ключами).

Рассмотрим общий алгоритм шифрования данных. Имеется открытый текст, который необходимо зашифровать и пароль. При шифровании по определенному правилу из пароля формируется т.н. гамма шифра (она же хеш-сумма или ключ шифра), которая впоследствии хранится вместе с зашифрованными данными. С ее помощью шифруются данные, а также в последствии – аутентификация при дешифровании. Обычно используется 128, 256, 512 и 1024 битная гамма (в зависимости от семейства криптоалгоритма). *Военные особо секретные данные шифруют с гаммой порядка 1344 битов*. Текст шифруется блоками, зачастую используются 128 и 256-битные блоки. При шифровании каждого блока данные в нем по определенному правилу трансформируются, при этом на них накладывается гамма шифра, и только после этого блок данных перемешивается несколько раз – это называется проходами, тем самым обеспечивается алгоритм шифрования. Количество проходов также влияет на степень криптостойкости алгоритма.

Симметричные криптосистемы

Часто называются криптосистемами с секретным ключом. Используется один ключ, с помощью которого производится как шифрование, так и дешифрование с использованием одного и того же алгоритма симметричного шифрования. Этот ключ передается двум участникам взаимодействия безопасным образом до передачи зашифрованных данных. Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных.

Обобщенная схема симметричной криптосистемы выглядит так:



Симметричные алгоритмы

Этот тип алгоритмов используется как симметричными, так и асимметрич-ными криптосистемами.

Тип	Описание
DES (англ.: Date Encryption Standard)	Популярный алгоритм шифрования, используемый как стандарт шифрования данных правительством США, предназначен для защиты важной, но не секретной информации. Шифруется блок из 64 бит, используется 64-битовый ключ (но требуется только 56 бит), 16 проходов. Может работать в 4 режимах: - Электронная кодовая книга (ECB-Electronic Code Book) – обычный DES, использует два различных алгоритма. - Цепочечный режим (CBC-Cipher Block Chaining), в котором шифрование шифрование блока данных зависит от результатов шифрования предыдущих блоков данных. - Обратная связь по выходу (OFB-Output Feedback), используется как генератор случайных чисел. - Обратная связь по шифратору (CFB-Cipher Feedback), используется для получения кодов аутентификации сообщений.
3-DES или тройной DES (англ.: Triple DES)	64-битный блочный шифратор, использует DES три раза с тремя различными 56-битными ключами. Достаточно стоек ко всем атакам. Однако если стоит выбор – лучше выбрать Blowfish, Twofish или Rijndael.
Каскадный 3-DES	Стандартный тройной DES, к которому добавлен механизм обратной связи, такой как CBC, OFB или CFB. Очень стоек ко всем атакам.
FEAL (быстрый алгоритм)	Блочный шифратор, используемый как альтернатива DES. Вскрыт, хотя после этого были предложены новые версии.
IDEA (Международный Алгоритм Шифрования, англ.: International Date Encryption Algorithm)	64-битный блочный шифратор, 128-битовый ключ, 8 проходов. Предложен недавно. До сих пор не прошел полной проверки, чтобы считаться надежным. Работает в 2 раза быстрее DES и считается значительно более криптостойким, чем DES как из-за длины ключа, так и из-за внутренней структуры.

Тип	Описание
Skipjack	Разработано АНБ в ходе проектов правительства США "Clipper" и "Capstone". До недавнего времени был секретным, но его стойкость не зависела только от того, что он был секретным. 64-битный блочный шифратор, 80-битовые ключи используются в режимах ECB, CFB, OFB или CBC, 32 прохода.
RC2	64-битный блочный шифратор, ключ переменного размера. Приблизительно в 2 раза быстрее, чем DES. Может использоваться в тех же режимах, что и DES, включая тройное шифрование. Конфиденциальный алгоритм, владельцем которого является RSA Data Security.
RC4	Потоковый шифр, байт-ориентированный, с ключом переменного размера. Приблизительно в 10 раз быстрее DES. Конфиденциальный алгоритм, которым владеет RSA Data Security.
RC5	Имеет размер блока 32, 64 или 128 бит, ключ с длиной от 0 до 2048 бит, от 0 до 255 проходов. Быстрый блочный шифр. Алгоритм, которым владеет RSA Data Security.
CAST	64-битный блочный шифратор, ключи длиной от 40 до 256 бит, 8 проходов. Неизвестно способов вскрыть его иначе как путем прямого перебора.
Blowfish	64-битный блочный шифратор, ключ переменного размера 32, 48, 56, 128 и 448 бит, 16 проходов, на каждом проходе выполняются перестановки, зависящие от ключа, и подстановки, зависящие от ключа и данных. Быстрее, чем DES примерно в 20 раз. Разработан для 32-битных машин.
Twofish	Был разработан автором Blowfish для соревнования NIST[а], где и выиграл, получив титул нового национального стандарта шифрования данных и вообще считается превосходящим Blowfish по стойкости и скорости. Есть два варианта: 128 и 256-битный ключ.
Rijndael	Этот алгоритм был отобран конкурсом NIST в октябре 2000 г, и стал новым официальным стандартом AES[§], используемый правительством США. Ключ в 128 и 256 бит. В отличие от Blowfish и Twofish требует большего времени для шифрования с большими ключами. 256-битная версия примерно на 40% медленнее 128-битной версии.

Тип	Описание
ГОСТ 28147-89	256-битный ключ (плюс 384 бита значений подстановок), размер блока – 64 бит, режимы: ECB, гаммирования, CFB; правильный выбор значений подстановок является коммерческой тайной (не все они хороши); является одним из самых стойких и не имеет ограничений по степени секретности информации.
Устройство с одноразовыми ключами (одноразовый блокнот)	Шифратор, который нельзя вскрыть. Ключом (который имеет ту же длину, что и шифруемые данные) являются следующие **n**-бит из массива случайно созданных бит, хранящихся в этом устройстве. У отправителя и получателя имеются одинаковые устройства. После использования биты разрушаются, и в следующий раз используются другие биты.
Поточные шифры	Быстрые алгоритмы симметричного шифрования, обычно оперирующие битами (а не блоками бит). Разработаны как аналог устройства с одноразовыми ключами, и хотя не являются такими же безопасными, как оно, по крайней мере практичны.

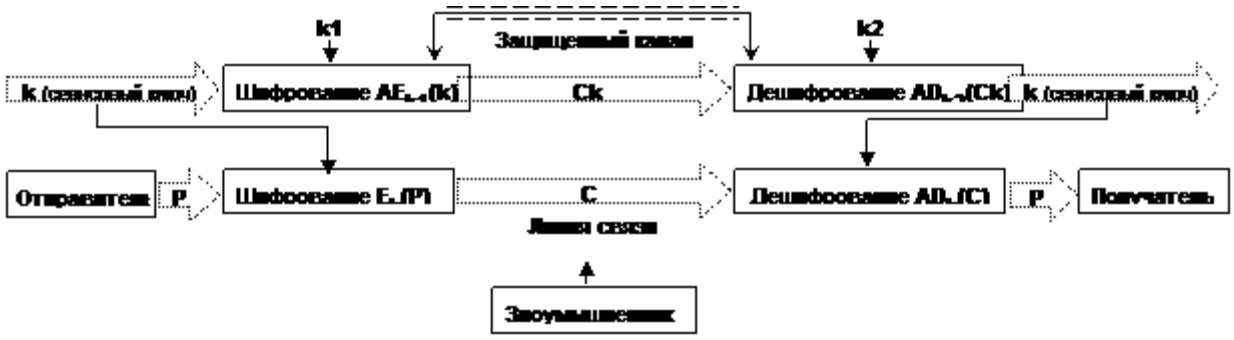
Асимметричные криптосистемы

Часто называются криптосистемами с открытым ключом. В ней ключи для шифрования и дешифрования разные и взаимосвязаны, хотя и создаются вместе. Один ключ **k1** – открытый, делается известным всем и используется для шифрования данных. Другой **k2** – закрытый, держится в тайне и используется для дешифрования данных. Хотя можно шифровать и дешифровать обоими ключами, данные, зашифрованные открытым ключом, могут быть правильно расшифрованы только закрытым ключом. Все асимметричные криптосистемы являются объектом атак путем прямого перебора ключей, и поэтому в них должны использоваться гораздо более длинные ключи, чем те, которые используются в симметричных криптосистемах, для обеспечения эквивалентного уровня защиты. Это сразу же сказывается на вычислительных ресурсах, требуемых для шифрования, т.е. попросту увеличивается время, необходимое на шифрование данных, хотя алгоритмы шифрования на эллиптических кривых могут смягчить эту проблему.

Для того чтобы избежать низкой скорости алгоритмов асимметричного шифрования, генерируется временный симметричный ключ (сеансовый) **k** для каждого сообщения. Само сообщение шифруется с использованием этого временного сеансового ключа и симметричного алгоритма шифрования/дешифрования. Затем этот сеансовый ключ шифруется с помощью открытого асимметричного ключа получателя и асимметричного алгоритма шифрования. После этого этот зашифрованный сеансовый ключ вместе с зашифрованным сообщением передается получателю. Получатель

использует тот же самый асимметричный алгоритм шифрования и свой закрытый ключ для расшифровки сеансового ключа, а полученный сеансовый ключ используется для расшифровки самого сообщения.

В асимметричных криптосистемах важно, чтобы сеансовые и асимметричные ключи были сопоставимы в отношении уровня безопасности, который они обеспечивают. Если используется короткий сеансовый ключ (например, 40-битовый DES), то не имеет значения, насколько велики асимметричные ключи. Хакеры будут атаковать не их, а сеансовые ключи. Асимметричные открытые ключи уязвимы к атакам прямым перебором отчасти из-за того, что их тяжело заменить. Если атакующий узнает секретный асимметричный ключ, то будет скомпрометировано не только текущее, но и все последующие взаимодействия между отправителем и получателем. Данная криптосистема используется в реализации PGP-ключей. Общая схема асимметричной криптосистемы выглядит так:



Асимметричные алгоритмы

Асимметричные алгоритмы используются в асимметричных криптосистемах для шифрования симметричных сеансовых ключей, которые в свою очередь используются для шифрования самих данных.

Более подробно с научной стороны с ассиметричными алгоритмами можно ознакомиться в книге Арто Саломаа, "Криптография с открытым ключом", Москва "Мир" 1995.

Тип	Описание
RSA	Популярный алгоритм асимметричного шифрования, стойкость которого зависит от сложности факторизации больших целых чисел. Называется по первым фамилиям авторов (Rivest-Shamir-Adleman). Лег в основу системы PGP (англ.: Pretty Good Privacy – Вполне хорошая секретность), реализованной под множество платформ, в том числе и под все операционные системы для IBM PC. С самого появления этой системы, спецслужбы США тщетно пытались бороться с ее распространением. Против Фила Циммермана (Phil Zimmerman), автора PGP, было возбуждено, а потом закрыто ("без комментариев") уголовное дело. Время от времени распространяется слух о том, что в очередную версию PGP вложена "закладка", позволяющая третьим лицам читать сообщения, зашифрованные PGP.
DSA	Переменная длина ключа до 1024 бит; ANSI X9.30-1.
ECC (криптосистема на основе эллиптических кривых)	Использует алгебраическую систему, которая описывается в терминах точек эллиптических кривых, для реализации асимметричного алгоритма шифрования. Является конкурентом по отношению к другим асимметричным алгоритмам шифрования, так как при эквивалентной стойкости использует ключи меньшей длины и имеет большую производительность. Современные его реализации показывают, что эта система гораздо более эффективна, чем другие системы с открытыми ключами. Его производительность приблизительно на порядок выше, чем производительность RSA, Диффи-Хеллмана и DSA.
Эль-Гамаль	Вариант Диффи-Хеллмана, который может быть использован как для шифрования, так и для электронной подписи.
ГОСТ Р 34.10-94	Напоминает DSS, но более устойчив за счет больших значений параметров.

Цифровая подпись

Для подписания документа отправитель шифрует его секретным ключем (на практике, для экономии времени шифруется контрольная сумма документа, что также позволяет поставить несколько подписей), получатель может дешифровать его (ее) с помощью открытого ключа отправителя. Подписанный документ может быть дополнительно зашифрован открытым ключом получателя (но нельзя подписывать зашифрованные сообщения!). Пары ключей для подписи и шифрования могут быть различными, хотя распространенные ассиметричные алгоритмы позволяют использовать одну и ту же пару для обеих целей (это уменьшает стойкость протокола).

Тип	Описание
DSS	Ассиметричный алгоритм шифрования DSA; стандарт США, 1994; медленный.
RSA	Ассиметричный алгоритм шифрования RSA, PKCS 1 в сочетании с MD2 или MD5.

Кроме протокола цифровой подписи требуется определить процедуру разбора конфликтных ситуаций (арбитр запрашивает секретный ключ и определяет виновного: подписант, получатель или центр сертификации открытых ключей).

Криптографически стойкие контрольные суммы (MAC, хеш, дайджест)

Необходимы для проверки целостности данных (при современных скоростях и объемах CRC-32 уже недостаточно) и цифровой подписи. Используются также для упрощения визуального сравнения открытых ключей (fingerprint). Криптографическая стойкость означает трудоемкость модификации сообщения с сохранением контрольной суммы или генерация сообщения, порождающего указанную контрольную сумму. В частности, длина контрольной суммы не должна быть менее 128 бит, а лучше 160. HMAC (RFC 2104) – сочетание любой криптографически стойкой контрольной суммы (не менее 128 бит) и шифрования при передаче хеша вместе с сообщением.

Тип	Описание
MD2	128 бит, медленный, RFC 1319.
MD4	128 бит, быстрый, RFC 1320, имеет известные дефекты.
MD5	128 бит, улучшенный (за счет скорости) MD4, RFC 1321; слабая устойчивость к коллизиям, хотя алгоритм генерирования коллизий неизвестен.
SHA, SHA-1	Проблема коллизий исправлена в версии SHA-1. 160 бит; стандарт США (ANSI X9.30-2, FIPS 180, FIPS 180-1), ISO/IEC 10118; на основе MD4, максимальная длина сообщения – 2^{64}.
ГОСТ Р 34.11-94	256 бит (на основе алгоритма шифрования ГОСТ 28147-89).

Советы по шифрованию данных

- Не используйте неизвестные криптоалгоритмы и программные комплексы шифрования.

- При выборе криптоалгоритма учитывайте его параметры. Из симметричных автор предпочитает использовать Rijndael, однако его вполне заменят MARS, RC6, Cast-256, Twofish или в крайнем случае ГОСТ 28147-89. Из асимметричных признанным считается RSA (исп. в PGP), но заменим DSA или ECC.

- Гамма шифра. Для симметричных крптоалгоритмов минимум 256 бит, а лучше 512 бит (если это позволяет используемый вами алгоритм). Например, 128-битный ключ имеет 3,4 x 10^{38} возможных вариантов. Т.е. он в 10^{21} раз более устойчив, чем 56-битный ключ DES.

- Блоки данных. Не менее 128 бит. Если блоки маленькие – степень перемешивания данных, а соответственно и степень криптостойкисти, зависит от количества проходов.

- Количество проходов. Вполне достаточно 32, можно 64.

- Применяйте последовательное шифрование несколькими различными криптоалгоритмами с разными паролями. Это уменьшит вероятность вскрытия защищаемой информации и/или, в крайнем случае, увеличит время ее вскрытия.

Примечание. Выбор более криптостойких алгоритмов влечет за собой увеличение времени шифрования/дешифрования данных. Поэтому перед выбором алгоритма стоит определиться в степени секретности ваших данных. Даже если они супер-секретны, при необходимости спецслужбы их все равно взломают. Если данные секретные и имеют небольшой размер – смело используйте самый "крутой" алгоритм, иначе подумайте о времени, которое вы будете тратить на их дешифрование при желании их просмотреть…

Стеганография или еще один шаг на пути ЗИ

Когда в V веке до н.э. тиран Гистий, находясь под надзором царя Дария в Сузах, должен был послать секретное сообщение своему родственнику в анатолийский город Милет, он побрил наголо своего раба и вытатуировал послание на его голове. Когда волосы снова отросли, раб отправился в путь. Так Геродот описывает один из первых случаев применения в древнем мире стеганографии – искусства скрытого письма.

Искусство развивалось, превратившись в науку, помогавшую людям на протяжении многих веков скрывать от посторонних глаз сам факт передачи информации. Еще древние римляне писали между строк невидимыми чернилами, в качестве которых использовались фруктовые соки, моча, молоко и некоторые другие натуральные вещества. Их опыт не был забыт: наверное, многие помнят, как в советских школах детям рассказывали о вожде всех гегемонов, не к ночи будет помянут, который писал, кажется молоком, между строк обычного письма нечто важное своим соратникам. При нагревании невидимый текст проявлялся. Так что не будь стеганографии, возможно не было бы и октябрьского переворота. Уж лучше бы не было стеганографии… Но не будем о грустном. Во время второй мировой войны немцами применялась "микроточка", представлявшая из себя микрофотографию размером с типографскую точку, которая при увеличении давала четкое изображение печатной страницы стандартного размера. Такая точка или несколько точек вклеивались в обыкновенное письмо, и, помимо сложности обнаружения, обладали способностью передавать большие объемы информации, включая чертежи.

Распространение стеганографии во время войны и тотальная шпиономания вызвали появление многих цензурных ограничений, которые сегодня могут вызвать лишь улыбку. В США были запрещены к международной почтовой пересылке шахматные партии, инструкции по вязанию и шитью, вырезки из газет, детские рисунки. Запрещалось посылать телеграммы с указанием доставить определенный сорт цветов к определенной дате, а впоследствии американским и английским правительствами были запрещены вообще все международные телеграммы, касающиеся доставки и заказа цветов. Как обстояли дела с международной почтой в СССР, рассказывать думаю не надо.

Развитие компьютерной технологии и средств коммуникации сделали бесполезными подобные ограничения. Сегодня каждый может воспользоваться теми преимуществами, которые дает стеганография как в области скрытой передачи информации, что особенно полезно в странах, где существует запрет на стойкие средства криптографии, так и в области защиты авторских прав. Те, кто интересются более подробной информацией о стеганографии, могут отправиться сюда http://www.petitcolas.net/fabien/steganography/. Мы же окинем взглядом практические применения этой науки.

По сути компьютерная стеганография базируется на следующих двух принципах:

1. Файлы, содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери функциональности, в отличие от других типов данных, требующих абсолютной точности.

2. Неспособность органов чувств человека различить незначительные изменения в цвете изображения или качестве звука, что особенно легко использовать применительно объекту, несущему избыточную информацию, будь то 16-битный звук, 8-битное или еще лучше 24-битное изображение. Если речь идет об изображении, то изменение значений наименее важных битов, отвечающих за цвет пиксела, не приводит к сколь-нибудь заметному для человека изменению цвета.

Обычно перед тем как информация скрывается от посторонних глаз – стеганографируется, она еще и шифруется криптоалгоритмами, тем самым уменьшается вероятность взлома защищаемых данных.

Цифровые водяные знаки как вариант Стеганографии

Если рассматривать коммерческие приложения стеганографии, то одним из наиболее перспективных направлений ее развития видится digital watermarking, т.е. создание невидимых глазу водяных знаков для защиты авторских прав на графические и аудио файлы. Такие помещенные в файл цифровые водяные знаки могут быть распознаны специальными программами, которые извлекут из файла много полезной информации: когда создан файл, кто владеет авторскими правами, как вступить в контакт с автором и т.п. При том повальном воровстве, которое происходит в Интернете, польза этой технологии очевидна.

Сегодня на рынке существует довольно много фирм, предлагающих продукты для создания и детектирования водяных знаков. Один из лидеров – фирма Digimarc (http://www.digimarc.com/), программы которой, если верить предоставленной самой фирмой информации, установили себе более миллиона пользователей. Фирма предлагает сгрузить с сайта PictureMarc, подключаемый модуль для Photoshop и CorelDraw, или отдельно стоящий ReadMarc. Дальше все просто: открываем в любимой программе графический файл и считываем скрытую информацию, если она, конечно, там есть. Можно получить и свой индивидуальный Creator ID (сроком на один год – бесплатно) и подписывать собственные опусы перед из размещением в сети, что и делают многочисленные клиенты: дизайнеры, художники, онлайновые галереи, журнал Плейбой. А дальше продукт для корпоративных пользователей MarcSpider будет ползать по паутине, просматривая все картинки, и сообщать владельцу об их незаконном использовании. Мне правда сложно представить, чтобы кто-то мог позариться на картинки из Плейбоя и разместить их у себя на сайте с коммерческой целью, поскольку привлечь они могут только детей младшего школьного возраста, но это уже личное дело издателей.

Казалось бы, наступает золотая эра честности, авторы больше не страдают от воровства, воры берут в руки фотоаппараты, кисти, мыши и учатся творить прекрасное в Photoshop'е… и вот тут некритичность файлов с изображениями к некоторым видоизменениям играет с ними плохую шутку. Несмотря на все заверения создателей соответствующих продуктов, цифровые водяные знаки оказались нестойкими. Они могут перенести многое – изменение яркости и контраста, использование спецэффектов, даже печать и последующее сканирование, но они не могут перенести хитрое воздействие специальных программ-стирателей, как StirMark (http://www.cl.cam.ac.uk/users/fapp2/steganography/image_watermarking/stirmark/) и UnZign (http://www.altern.org/watermark/), которые вскоре появились в Интернете, причем очевидно не с целью насолить фирме Digimarc, Signum Technologies (http://www.signumtech.com/) и другим, а для того, чтобы дать пользователям возможность сделать правильный выбор, основываясь на независимой оценке стойкости водяных знаков. А оценка эта на сегодняшний день малоутешительна – водяные знаки всех производителей уничтожаются без заметного ухудшения качества изображения.

Невосстановимое удаление данных

Пресса и Интернет полны сообщениями о случайно приобретенных компьютерах (при распродаже имущества ликвидируемых компаний), на жестких дисках которых осталась конфиденциальная информация: персональные данные сотрудников (номера лицевых счетов в банке, кредитных карточек, карт социального обеспечения, размер заработной платы), бухгалтерские и другие внутренние документы, материалы совещаний советов директоров. Конфиденциальная информация должна не только храниться с соблюдением строгих правил, но и надежно уничтожаться! Удаление файлов данных средствами операционной системы,

форматирование разделов жестких дисков и их удаление не гарантируют невозможности восстановления информации специальными программными или аппаратными средствами. Гарантированное уничтожение конфиденциальной информации возможно только с помощью специально разработанных программ, реализующих зачастую довольно сложные алгоритмы.

Как известно, данные записываются и хранятся на жестком диске в виде отдельных секторов – небольших участков диска. Сектора одного файла могут быть хаотически разбросаны по поверхности диска, а могут идти подряд. В начале жесткого диска находится т.н. FAT-таблица[а], которая содержит список файлов, а также отдельно для каждого файла – последовательный список секторов, в которых находятся данные файла. При удалении файла – все сектора файла помечаются как пустые (в которые можно записать новые данные), а запись о файле стирается из FAT. Иными словами, удалив файл, вы стираете лишь запись, которая указывала, где он находится. Это еще одна лазейка для спецслужб обнаружить у вас запрещенную информацию. Практически же имеются системы восстановления утерянных/удаленных данных, свободно работающие как с FAT так и NTFS файловыми системами и доступные для использования обычным пользователям *(см. "Восстановление удаленных данных" PAGEREF Восстановление_удаленных_данных \p \h на стр. 297)*. Однако эти системы полноценны лишь в том случае, если на место удаленного файла не была записана другая информация. Учитывая сегодняшний спрос на жесткие диски с размером более 40 Гб, на диске со средней интенсивностью использования можно найти информацию месячной, а то и более давности (личный опыт). Хотя эта вещь случайная. Можно навсегда потерять информацию, которую удалил 3 минуты назад, одним запуском любимого Unreal Tournament. Тоже самое относится и к программным копмплексам восстановления данных после форматирования раздела жесткого диска.

Невосстановимое форматирование разделов

Аналогично вышеописанному при форматировании разделов диска перезаписываются только заголовочные структуры диска (напр. FAT-таблица), которые хранят данные о разделе и положении файлов на диске, при этом сами данные остаются.

Пару слов об Интернете

Как известно, вначале Интернет был чисто студенческой разработкой в США, затем ним заинтересовались военные. Ну а сейчас вы видите во что это превратилось. Как говорит Алексей – огромная помойная яма и немного "зефира". Ну да ладно, не будем о грустном…

Технология Интернета основана на сетевых принципах TCP/IP протокола. В общем это выглядит следующим образом. Есть множество веб-серверов, на которых выложена некоторая информация, доступная пользователям сети Интернет с соответствующими правами на доступ к ней. Есть сервера провайдеров, которые вместе с веб-серверами образуют глобальную сеть. Провайдеры предоставляют конечным пользователям

интернета доступ к Интернету любым из возможных способов – диал-ап соединение (модем), радио-эзернет (радио-связь), выделенная линия (прямое кабельное соединение) и т.п. Таким образом сервера провайдеров являются как бы связующим звеном между конечным пользователем и сетью Интернет и одновременно шлюзом, т.к. на этих серверах установлены прокси-сервера – специальное программное обеспечение для фильтрования траффика, управления доступом пользователей к ресурсам Интернета и многое другое. Например, с помощью прокси-сервера, можно запретить Васе Пупкину доступ к электронной почте или ICQ, а использование Интернета свести к временному интервалу с 9.00 до 12.00 с пропускной способностью канала не более 8К/сек.

Еще одной важной и неприятной особенностью прокси-серверов является ведение журналов событий. Как известно каждый ПК в сети характеризуется т.н. IP-адресом, уникальным номером внутри конкретной подсети, в которую он входит. Каждый пользователь, подключаясь к серверу провайдера, оставляет свой "след" в журнале событий прокси-сервера. В зависимости от настроек аудита прокси-сервера в журнале событий может храниться информация начиная с даты и веремени подключения/отключения и заканчивая подробным списком файлов, которые вы скачивали (в частном случае адреса посещенных web-страниц). Обязательным пунктом в прокси-серверах у провайдеров является аутентификация (если бы ее не было – каждый пользователь мог бы свободно получить доступ к Интернету), данные которой также заносятся в журнал событий.

Последний факт не может радовать пользователей сети, особенно если вы совершаете в Интернете некие "противозаконные" действия. Конечно же для неопытных пользователей существует альтернатива в виде прозрачных или анонимных прокси-серверов, которые якобы скрывают информацию о пользователе (в частном случае его реальный IP-адрес и т.п.) и/или не ведут журналы событий. Т.е. прозрачный прокси-сервер подменяет ваш реальный IP-адрес другим или вообще не показывает его для Web-серверов. Позволю сразу же опротестовать это и высказать свой взгляд на эту проблему:

1. Складывается впечатление, что все прозрачные прокси-сервера специально запущены в работу спец-службами, а информация об их безопасности и надежности распространена преднамеренно.

2. Даже если они функционируют не под патронажем спец-служб, последние без особых трудностей получат информацию о вас от администратора подобного сервера.

Так что как бы вы не пытались скрытся, увы – это практически невозможно. А даже если и возможно, то на это требуется слишком много усилий и это удел профессионалов.

Вышеприведенное касается внешней стороны Интернет-соединения. Однако кроме этого есть еще небольшая проблема внутри системы. Дело в том, что в Windows предусмотрен т.н. журнал посещенных страниц. В нем хранятся все посещенные вами web-страницы (однако это зависит от настроек в броузере). Также имеется папка временных файлов Интернета.

Используется для ускорения последующего просмотра посещенных страниц Интернета. В этой папке могут быть непосредственные доказательства ваших "грешков". Например, даже если вы заявляете о сфабрикованности журнала событий провайдера, у вас легко могут найти улики среди временных файлов (если они конечно же не удалены оттуда или вообще туда не сохранялись). Сохранение страниц в эту папку следует отменить, если безопасность для вас прежде всего. Еще одной негативной чертой являются Cookie-файлы. Они используются для хранения личной информации о вас некоторыми web-страничками, которые вы просматриваете. В основном там хранятся данные аутентификации. Еще одним следом является список автозаполнения форм и список предыдущего поиска (хотя ним обычно не пользуются).

[a] Системный администратор – он же суперпользователь. Имеет безграничные права доступа к системе и ее ресурсам.

§ Метод перебора – ручной или програмный перебор всех возможных комбинаций паролей, не обязательно по порядку.

ШТАТ ВИКТОРИЯ, АВСТРАЛИЯ: НАЧАТО ОБСУЖДЕНИЕ ПЕРЕЧНЯ ДОКУМЕНТОВ С УКАЗАНИЕМ СРОКОВ ХРАНЕНИЯ ДЛЯ УЧРЕЖДЕНИЙ И ПОДРАЗДЕЛЕНИЙ ВЫСШЕГО ОБРАЗОВАНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Источник: сайт PROV
http://prov.vic.gov.au/government-recordkeeping/request-for-feedback-retention-and-disposal-authority-for-records-of-the-higher-and-further-education-functions
Автор: Наташа Храмцовская

Управление государственных документов штата Виктория (PROV) предлагает заинтересованным сторонам принять участие в обсуждении нового проекта перечня документов с указанием сроков хранения и действий по их истечении для сферы высшего образования и повышения квалификации.

Цель этого документа, предыдущая редакция которого была опубликована в виде стандарта, заключается в том, чтобы перечислить обязательные виды документов, относимые к числу архивных документов штата, и обеспечить правовую основу для уничтожения документов, не подлежащих постоянному хранению, по истечении соответствующих сроков хранения.

Проект перечня, а также краткий отчет, содержащий положенные в основе перечня сведения, описание сферы его применения и рекомендации по проведению экспертизы ценности доступны по адресам:

- Проект перечня, http://prov.vic.gov.au/wp-content/uploads/2016/06/Draft-Higher-Ed-RDA-for-external-feedback-20060624.pdf
- Отчет, http://prov.vic.gov.au/wp-content/uploads/2016/06/Higher-Ed-RDA-Appraisal-scope-report-20160621.pdf

Мы будем благодарны за замечания и предложения по следующим вопросам:

- Являются ли сроки хранения разумными?
- Достаточно ли ясным языком написан перечень?
- Видите ли Вы какие-либо пробелы в перечне?

Просьба присылать Ваши замечания и предложения по адресу agency.queries@prov.vic.gov.au.

Мой комментарий: Думаю, что и в наших условиях публичные обсуждения разрабатываемых перечней (действительно публичные, а не «междусобойчики» в узком кругу «своих» людей) были бы очень полезными, поскольку именно реально работающие с документами люди знают многие тонкости и проблемы, о которых тот же ВНИИДАД даже не подозревает.

ИСПАНИЯ: СЕРТИФИЦИРОВАННАЯ ОЦИФРОВКА СЧЕТОВ-ФАКТУР, ИЛИ ОБ ОПЫТЕ ЗАМЕЩАЮЩЕГО СКАНИРОВАНИЯ

Источник: блог Todo es electrónico https://inza.wordpress.com/2016/07/17/certified-digitization-of-invoices/

Автор: Наташа Храмцовская

Статья Хулиана Инзы (была опубликована 17 июля 2016 года на его блоге «Todo es electrónico» («Всё электронное»).

В Испании «сертифицированная оцифровка счетов-фактур» - это компьютерный процесс, позволяющий получить верные электронные копии счетов-фактур, имеющие равную юридическую силу с их бумажными оригиналами, - и, как следствие, **действующее законодательство позволяет уничтожать бумажные оригиналы оцифрованных счетов-фактур**. Соответствующая компьютерная среда должна включать защищённую базу данных, обеспечивающую пользователям и аудиторам возможность мгновенного доступа и извлечения любого счета-фактуры для целей проведения налоговой проверки или аудита.

Использование электронных счетов-фактур регламентируется Королевским декретом (Real Decreto, RD) 1619/2012 от 30 ноября 2012 года «Об утверждении регламента, регулирующего обязательства по работе со счетами-фактурами» (*Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación*, https://www.boe.es/boe/dias/2012/12/01/pdfs/BOE-A-2012-14696.pdf), вместе с рядом положений, установленных Приказом Министерства экономики EHA/962/2007 от 10 апреля 2007 года «О реализации отдельных положений, касающихся использования электронных счетов-фактур и их хранения в электронном виде, содержащихся в Королевском декрете RD 1496/2003 от 28 ноября 2003 года об утверждении положения, о выставлении счетов-фактур» (*Orden EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el reglamento por el que se regulan las obligaciones de facturación*, https://www.boe.es/boe/dias/2007/04/14/pdfs/A16451-16458.pdf).

Королевский декрет RD 1496/2003 (см. http://www.boe.es/boe/dias/2003/11/29/pdfs/A42537-42556.pdf) был отменен декретом RD 1619/2012, однако разработанные в период его действия правила по-прежнему действуют.

Согласно упомянутому декрету RD 1619/2012, изначально-электронные и оцифрованные счета-фактуры и должны быть подписаны электронной подписью. «Это должна быть действительная квалифицированная электронная подпись, соответствующая положениям статьи 3.3 закона 59/2003 от 19 декабря 2003 года об электронной подписи» (*см. Ley 59/2003, de 19 de diciembre, de firma electrónica*, https://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf).

Квалифицированной является усиленная электронная подпись на основе квалифицированного сертификата, **сформированная при помощи защищенного устройства для создания подписи** (*Выделенною мною положение отличает «нашу» квалифицированную подпись от «их», и российские подписи по европейским меркам - это не квалифицированные подписи, а «усиленные электронные подписи на основе квалифицированного сертификата» - Н.Х.*).

Опубликованное 1 ноября 2007 года в официальном государственном бюллетене (BOE) Постановление налоговой службы (Agencia Estatal de Administración Tributaria, AEAT) от 24 октября 2007 года «О порядке одобрения программного обеспечения, используемого для сертифицированной оцифровки в соответствии с приказом EHA/962/2007 (*Resolución de 24 de octubre de 2007, de la Agencia Estatal de Administración Tributaria, sobre procedimiento para la homologación de software de digitalización contemplado en la Orden EHA/962/2007, de 10 de abril de 2007*, https://www.boe.es/boe/dias/2007/11/01/pdfs/A44614-44615.pdf), требует: чтобы программное обеспечение для оцифровки было одобрено, приложение

должно быть представлено директору департамента налоговой информации любого из регистрирующих офисов.

Согласно ст. 8 Постановления, заявитель должен представить декларацию о соответствии, в которой указать, что программное обеспечение соответствует требованиям законодательства, и приложить к ней ряд документов:

- Техническую документацию, описывающую программное обеспечение;
- Отчет аудитора об оценке программного обеспечения,
- План менеджмента качества,
- CD-R диск с информацией в электронном формате и **CD-R диск с копией программного обеспечения**.

Если документация и программное обеспечение признаются соответствующими нормативным требованиям, то выдается официальное разрешение, содержащее присвоенный ссылочный код, который в дальнейшем должен включаться в каждый оцифрованный счет-фактуру в качестве метаданных.

После одобрения налоговой службой (AEAT) программного обеспечения для сертифицированной оцифровки, полученный с его помощью и подписанный электронной подписью графический образ **для налоговых целей** признается равносильным бумажному счету-фактуре.

В процессе сертифицированной оцифровки используются фотоэлектрические методы, подобные тем, что применяются в сканерах и цифровых фотоаппаратах, для преобразования изображения на бумажном документе в электронный образ в одном из широко распространенных стандартных форматов, с разрешением не менее 200 точек на дюйм (в соответствии с информацией, размещенной на веб-сайте AEAT).

Как следствие, может быть авторизовано уничтожение больших объёмов бумажных оригиналов, что дает экономию как в плане управления делами и документами, так и в плане сокращения косвенно связанных с налоговой отчетностью расходов.

Испанская юридическая и техническая среда для использования электронных счетов-фактур и сертифицированной оцифровки (включая электронную подпись) описана в книге **на английском языке** «Электронные счета-фактуры» (Electronic invoicing,

https://inza.files.wordpress.com/2011/08/manual-factura-electronica-ingles-english-handbook-electronic-invoicing-v2010.pdf).

Хотя эта книга была выпущена в 2010 году, она в основном сохраняет свою актуальность (не считая сравнительно незначительных изменений, связанных с внесенными в законодательство с 2010 года изменениями).

Мой комментарий: Думаю, испанский опыт можно перенести и на нашу почву. С моей точки зрения, при решении в России вопроса о замещающем сканировании бумажных документов (т.е. с последующим уничтожением оригиналов) нереально надеяться на то, что это будет позволено везде и всюду. Соответственно, я не слишком верю в успешность начатых этой весной усилий по придумыванию поправок в действующее законодательство, которые позволили бы переводить в электронный вид широкий круг используемых в деловой деятельности документов.

Можно, однако, договориться с заинтересованными государственными органами о том, что будет дозволено замещающее сканирование конкретных видов документов, для применения электронных копий в конкретных целях – при условии соблюдения установленных требований (и, скорее всего, при наличии дополнительных мер контроля).

ЗМІСТ