Содержание:

Введение

Курс "Введение в защиту информации от внутренних ИТ-угроз" посвящен постановке задач по предотвращению реализации внутренних ИТ-угроз – изменению, уничтожению и хищению информации легальными пользователями. В этом курсе слушатель научится определять "болевые точки" информационных систем и оценивать необходимость сочетания различных технологических решений и организационных методов борьбы с внутренними ИТ-угрозами.

Статистический анализ показывает, что внутренние ИТ-угрозы находятся в лидерах информационных угроз, отодвинув на второй план традиционных лидеров – хакерские атаки и вирусы. Это связано с несколькими причинами. Первая – успех производителей средств защиты от внешних угроз и повсеместное распространение их продуктов. Антивирусные компании и производители межсетевых экранов и систем обнаружения вторжений предлагают продукты, на которых можно построить гибкую многоуровневую защиту информационных систем. Успехи в биометрии и других системах аутентификации позволяют построить удобную и эффективную систему защиты от несанкционированного доступа, включающую единую точку входа и контроль над учетными записями. Вся концепция информационной безопасности строится на разделении прав доступа к ИТ-ресурсам на "санкционированные" и "не санкционированные".

Приблизившись к решению проблемы защиты периметра информационной системы снаружи, производители средств информационной безопасности оставили без внимания то, что делает пользователь с "санкционированным" доступом. Вендоры программного и аппаратного обеспечения, словно сговорившись, увеличивают количество каналов, портов и протоколов, по которым легальный пользователь может похитить информацию – системы становятся все более дружелюбными к пользователю. Беспроводные протоколы IrDA, Bluetooth и WiFi, сменные носители (от традиционных flash-носителей до медиа-плееров и фотокамер), программы синхронизации мобильных телефонов и PDA, позволяют достаточно легко

передавать огромные объемы информации. Доступ к высокоскоростным каналам Интернет, постоянно растущий объем файлов, которые возможно присоединять к почтовым и IM сообщениям позволяют пересылать большие объемы информации.

1. Электронная подпись

Электронная подпись (ЭП) — это специальный реквизит, который превращает обычный файл с информацией в юридически значимый документ. Такая подпись — полный аналог собственноручно поставленного автографа.

Согласно закону № 64-ФЗ от 6 апреля 2011 года «Об электронной подписи», заверенные ею электронные документы становятся равнозначными подписанным бумагам. Они используются внутри компании, передаются контрагентам и направляются в контролирующие органы. При этом представление аналогичного документа «на бумаге» не требуется.

1.1. Зачем нужна электронная подпись

Назначение электронной подписи в следующем:

1. удостоверить личность подписанта;
2. подтвердить, что документ является юридически значимым;
3. гарантировать, что после подписания документ не был изменен.

Сейчас очень популярно регистрировать онлайн: процедура требует наличия ЭЦП. Также обычный пример использования электронной подписи — подача налоговой декларации. При направлении в бумажном виде ее нужно распечатать в двух экземплярах, заверить подписью директора и отвезти в ИФНС.

Это долго, трудоемко и неэффективно. Чтобы упростить процесс, можно выпустить ЭП и заключить договор с оператором электронного документооборота. И тогда подача декларации займет не более пары минут. Ее даже не нужно печатать — достаточно подписать при помощи ЭП и отправить в налоговую.

1.2. Как работает ЭП

С виду то, что принято называть электронной подписью, выглядит как обычный USB-накопитель. В действительности это не сама ЭП, а лишь инструмент для ее формирования. Этакий современный аналог обычной ручки. На накопителе содержится набор файлов:

- Программа для шифрования.
- Уникальный закрытый ключ шифрования.
- Сертификат, подтверждающий личность владельца ЭП, с открытым ключом, который применяется для расшифровки подписи.

Устройство подключается к компьютеру, затем производится несложная настройка рабочего места. После этого подпись готова к использованию. Обычно документы подписываются ЭП в приложении, через которое осуществляется их отправка. Например, в сервисе электронного документооборота, личном кабинете на сайте государственного органа или же бухгалтерской программе, через которую направляются отчеты.

Процесс постановки электронной подписи кажется со стороны непонятным и сложным. В действительности же его можно описать в нескольких строках. В момент «подписания» документа ЭП происходит следующее:

- файл документа преобразуется в длинный набор символов — хеш;
- хеш шифруется при помощи закрытого ключа — это и есть электронная подпись;
- ЭП прикрепляется к документу, а вместе с ней — сертификат, в котором «зашита» информация о владельце подписи и ключ для расшифровки хеша.

На стороне получателя происходит следующее:

- проверяется владелец сертификата — так можно быть уверенным, что подпись принадлежит уполномоченному лицу;
- происходит подсчет хеша того электронного документа, который получен;
- при помощи открытого ключа происходит расшифровка ЭП — теперь известно, каков был хеш у отправленного файла;
- хеши сравниваются — они должны быть одинаковы.

Для чего нужна такая проверка? Она покажет, что документ целостный и подлинный. Если же злоумышленник решит исправить его уже после подписания, хеш файла изменится. При проверке он не сойдется с тем, который зашифрован в электронной подписи.

Это будет означать, что файл не является подлинным. Поэтому подписанные ЭП документы считаются защищенными от несанкционированного доступа. Надежный алгоритм шифрования позволяет передавать информацию через интернет без опасений.

Ведь даже если документ будет перехвачен, незаметно внести в него изменения не выйдет.

2. Новые формы ЭП. Формы и Виды

Простая подпись – это комбинации символов, коды и пароли, которые позволяют установить факт формирования электронной подписи определенным лицом. Такую подпись достаточно легко взломать.

Усиленная подпись (неквалифицированная и квалифицированная) формируется с помощью внешнего носителя – флэшки или дискеты. Дополнительная защита усиленной квалифицированной подписи – это ключ проверки ЭП, указанный в квалифицированном сертификате. Отчетность и юридически значимые документы должны подписываться только усиленной квалифицированной подписью.

Удостоверяющие центры предлагают разные электронные подписи в зависимости от возможности доступа к различным ресурсам. Так, ЭП для обычного физического лица всего за 450 рублей позволяет вести защищенный юридически значимый документооборот, получать государственные и муниципальные услуги онлайн, платить налоги через личный кабинет.

3. ЭП в системах электронного документооборота. Подпись для электронного документооборота (ЭДО)

Именно электронная подпись для ЭДО один из необходимых элементов, которые обеспечивают ему юридическую значимость. Электронная подпись в Диадоке — это только КЭП. Так удобнее для пользователей.

Электронный документооборот и электронная подпись тесно взаимосвязаны. Именно электронная подпись для ЭДО один из необходимых элементов, которые

обеспечивают ему юридическую значимость.

Термин «электронная цифровая подпись» стал неактуальным с тех пор, как прекратил действовать Закон «Об электронной цифровой подписи» и вступил в силу 63-ФЗ «Об электронной подписи». Сейчас корректно употреблять по отношению к электронным документам и документообороту словосочетание «электронная подпись». Она бывает разных типов.

Квалифицированная электронная подпись (КЭП) самодостаточна: документ, которым она подписана, по умолчанию обладает юридической силой.

Неквалифицированной электронной подписью (НЭП) также можно визировать документы, но потребуются еще гарантии в виде дополнительного соглашения между контрагентами. В нем должно быть оговорено, что стороны считают оригиналами документы, подписанные НЭП.

В любом из этих случаев подпись должна соответствовать требованиям 63-ФЗ «Об электронной подписи».

В ряде случаев электронные документы можно подписать только КЭП, иначе они не будут обладать юридической силой. Это счета-фактуры, универсальные передаточные документы, их исправленные и корректировочные пары.

Электронная подпись в Диадоке — это только КЭП. Так удобнее для пользователей. Во-первых, у подавляющего числа из них она уже имеется, так, как только ею можно подписывать электронную отчетность в ФНС. Во-вторых, с КЭП не нужно тратить время на заключение дополнительного соглашения об ЭДО с контрагентом.

Электронная подпись в системе электронного документооборота — необходимое условие для его законности и юридической значимости.

4. Принципы формирования ЭП. Формирование ЭП

Для успешного создания и использования ЭП электронного документа в современных условиях обмена электронными сообщениями и документами, в том числе в сетях общего пользования, необходимо, чтобы открытый ключ (в том числе и закрытый ключ) был соотнесен с лицом, создающим ЭП, а для его создания использовалось сертифицированное средство (специальное программное

обеспечение).

Для выполнения первого условия необходимо обратиться в центр сертификации.

Удостоверяющий центр или центр сертификации - это организация или подразделение организации, которая выпускает сертификаты ключей электронной подписи.

Сертификат открытого ключа удостоверяет принадлежность открытого ключа некоторому лицу. Сертификат открытого ключа содержит имя субъекта, открытый ключ, имя удостоверяющего центра (или центра сертификации), политику использования, соответствующего удостоверяемому открытому ключу закрытого ключа и другие параметры, заверенные подписью уполномоченного лица удостоверяющего центра.

Сертификат открытого ключа используется для идентификации субъекта и уточнения операций, которые субъекту разрешается совершать с использованием закрытого ключа, соответствующего открытому ключу, удостоверяемому данным сертификатом. Структура цифровых сертификатов, а также списков отозванных сертификатов (CRL), определяется стандартом X.509.

Заявитель обращается в удостоверяющий центр и представляет документы, необходимые для его идентификации (например, паспорт). Уполномоченный сотрудник УЦ выполняет проверку документов, после чего формируется пара ключей. Достоверность первого удостоверяется сертификатом, заверенным ЭП сотрудника УЦ. Секретный ключ на съемном носителе передается заявителю, который, расписываясь в получении сертификата и секретного ключа, обязуется никому не передавать секретный ключ, а в случае его утраты, обратиться в удостоверяющий центр для отзыва сертификата.

После получения закрытого ключа и сертификата открытого ключа, необходимо установить сертификат на компьютер, где будет создаваться электронная подпись. Процедура установки корневого сертификата удостоверяющего центра, а также личного сертификата с привязкой к секретному ключу, производиться с помощью средств операционной системы и специального программного обеспечения, обеспечивающего работу с сертификатом и закрытым ключом при выполнении операций шифрования и создания ЭП.

В операционных системах Microsoft Windows такое программное обеспечение получило название - криптопровайдер (Cryptography Service Provider, CSP).

Криптопровайдер - это независимый модуль, позволяющий осуществлять криптографические операции, управление которым происходит с помощью функций CryptoAPI . Проще говоря, криптопровайдер – это посредник между операционной системой и клиентской программой, предназначенной для выполнения уже вполне конкретных действий, например, шифрования данных или создания ЭП документа. Крипто-провайдер обычно устанавливается в систему в момент установки клиентской программы, поэтому этот сложный процесс не заметен для пользователя.

Также нужно отметить, что крипто-провайдеры поддерживающие различные зарубежные криптографические алгоритмы, поставляются вместе с операционной системой и не требуют отдельной установки. В частности, поэтому, для того чтобы подписать электронное сообщение в почтовой программе MS Outlook на сертификате выпущенном в вашей организации, Вам нужно только установить выпущенный сертификат на Ваш компьютер. Однако, полученную таким образом ЭП можно использовать только в рамках Вашей организации или группы компаний, имеющих внутреннее соглашение об использовании такой ЭП. Для обеспечения юридической значимости, т.е для того, чтобы полученная ЭП признавалась любыми другими гражданами и организациями, в том числе государственными органами, необходимо: во-первых, изготовить сертификат и получить секретный ключ в удостоверяющем центре (аккредитованном и имеющими необходимые лицензии ФСТЭК и ФСБ), во-вторых, использовать для изготовления ЭП специальное сертифицированное средство. Например, одним из таких средств является комплекс Крипто-АРМ производства ООО «Цифровые технологии», который должен использоваться вместе с сертифицированным крипто-провайдером, производства ООО «КРИПТО-ПРО».

После того, как на компьютере установлены сертификат, соответствующее средство изготовления ЭП и произведены необходимые настройки, можно легитимно применять ЭП.

При использовании электронной подписи для защиты документов она может передаваться несколькими способами. Конкретный вариант выбирается исходя из того, какие задачи решаются с ее помощью.

Присоединенная

В случае создания присоединенной подписи создается новый файл ЭП, в который помимо данных ЭП помещаются данные подписываемого документа. Этот процесс

аналогичен помещению документа в конверт и его запечатыванию. Перед извлечением документа следует убедиться в сохранности печати (для ЭП в ее правильности). К достоинствам присоединенной подписи следует отнести простоту дальнейшего манипулирования с подписанными данными, т.к. все они вместе с подписями содержатся в одном файле. Этот файл можно копировать, пересылать и т.п. К недостаткам следует отнести то, что без использования средств создания ЭП уже нельзя прочесть и использовать содержимое файла, точно так же, как нельзя извлечь содержимое конверта, не расклеив его.

Отсоединенная

При создании отсоединенной подписи файл подписи создается отдельно от подписываемого документа, при этом сам файл подписываемого документа никак не изменяется. Преимуществом отсоединенной подписи является то, что подписанный файл можно читать, не прибегая к средству создания ЭП. Недостаток отсоединенной подписи - необходимость хранения подписанной информации подписанного файла и одного или нескольких файлов с подписями.

Внутри данных

Применение ЭП этого вида существенно зависит от приложения, которое их использует, например, ЭП внутри документа Acrobat Reader. Вне приложения, создавшего ЭП, без знания структуры его данных проверить подлинность частей данных, подписанных ЭП затруднительно.

5.Правовые аспекты применения ЭП.

Понятие «электронная цифровая подпись». Традиционно для документирования в качестве материального носителя применялась писчая бумага. Созданный на таком носителе документ, подтвержденный соответствующими реквизитами и снабженный подписями, широко используется в гражданских, экономических и иных отношениях, в том числе и как доказательственный материал при судебном разбирательстве. Доказательственная способность документированной информации основана на возможности установления с помощью почерковедческой экспертизы того факта, что О V

данный конкретный документ является оригиналом и что подпись на нем с большой степенью вероятности принадлежит конкретному лицу.

С внедрением новых информационных технологий вместо бумаги в качестве материальных носителей стали использоваться машиночитаемые носители - магнитные и оптические диски, память ЭВМ, электрические колебания, электромагнитные волны, и возникло понятие «электронный документ». К сожалению, в отличие от информации, зафиксированной на бумажном носителе, информация на машиночитаемом носителе может быть легко изменена или скопирована без желания ее автора в результате несанкционированного доступа к ней постороннего лица, причем без всяких следов такого вмешательства. Естественно, в этом случае документ на машиночитаемом носителе теряет свою доказательственную способность, его легко подделать и никакая экспертиза не в состоянии эту подделку выявить.

Возникла проблема установления доказательственной силы электронного документа. Необходимо было создать такой механизм записи информации на нем, который, с одной стороны, исключал бы возможность несанкционированного доступа постороннего лица к информации с целью ее искажения или подделки, а с другой - позволял бы конкретному лицу ставить на этом документе некоторую отметку, аналогично его подписи на бумаге, которую было бы невозможно подделать, а экспертиза могла бы надежно подтвердить принадлежность этой отметки-подписи данному лицу.

Отсюда возникло понятие «электронная цифровая подпись» (ЭЦП), которая посредством специального программно-информационного комплекса обеспечивает надежное подтверждение оригинальности сведений, реквизитов документа и факта его «электронного подписания» конкретным лицом. Таким образом, электронная цифровая подпись обеспечивает ввод и передачу документа по системе связи и телекоммуникации с предоставлением возможности в любой точке трафика и в любой момент времени вывести этот документ из системы и представить его для решения спора.

В Гражданском кодексе Российской Федерации (п. 2 ст. 160) впервые

KJ

в российском законодательстве допускается использование электронной цифровой подписи при совершении сделок, но лишь в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашениями сторон. В Федеральном законе «Об информации, информационных технологиях и о защите информации» введено понятие «электронное сообщение как информация, переданная или

полученная пользователем информационно-телекоммуникационной сети» (ст. 2) и определяется его правовой статус. В соответствии с этим законом (ст. 11) электронное сообщение, подписанное электронной цифровой подписью (ЭЦП), признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными документами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано ЭЦП или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

Закон также определяет право получателя электронного сообщения, находящегося на территории РФ, проводить проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашениями сторон случаях получатель обязан проводить такую проверку.

Как видно из нормы этих статей, законодательство лишь подтверждает возможность использования ЭЦП, но не определяет правового режима ее использования (случаи и порядок ее использования). Поэтому необходимость принятия в Российской Федерации закона «Об электронной цифровой подписи» являлась очевидной и назревшей. Актуальность этого за- ключения подтверждается также работой, проводимой в странах Европейского Союза по созданию глобальной системы электронной коммерции. На совещании европейской комиссии по этим вопросам, состоявшемся в Брюсселе 29 июня 1998 г., были определены основные требования к национальному законодательству стран-участниц. В них, наряду с экономическими вопросами выделены законы о криптографической защите, об ЭЦП, о защите персональных данных и др.

30 ноября 1999 г. Еврокомиссия приняла законопроект о поддержке и применении ЭЦП во всех странах, входящих в Евросоюз. Министры по телекоммуникациям стран ЕС утвердили закон, который придает ЭЦП на контрактах, согласованных по Интернету, такой же юридический статус, как и их эквивалентам, сделанным от руки.

После довольно долгого обсуждения и доработки 10 января 2002 г. был подписан Федеральный Закон Российской Федерации «Об электронной цифровой подписи», положивший начало созданию правовой базы электронного документооборота в России.

Целью указанного Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых ЭЦП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. Его действие распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством РФ случаях.

Технология получения ЭЦП. Прежде чем рассмотреть суть закона, необходимо понять основные механизмы передачи электронных документов с использованием ЭЦП. В основе формирования ЭЦП лежит принцип шифрования передаваемого сообщения. При этом ключ, на котором шифруется информация, является «секретным» и известен только отправителю. Чтобы исключить возможность подделки, он, как и любой шифр-ключ, должен удовлетворять принятым в криптографии требованиям. В частности, должна быть исключена возможность подбора ключа. В современной криптографии для изготовления ключей используется специальное оборудование, позволяющее изготовить ключи, вероятность случайного подбора которых составляет величину порядка 10 70—10 80, т. е. практически подбор исключен. Каждому «секретному ключу» соответствует свой «открытый ключ», которым пользуются лица, принимающие сообщения. Открытый ключ, соответствующий конкретному секретному ключу, формируется отправителем сообщения с помощью специального программного обеспечения, заложенного в средства ЭЦП, и заранее рассылается другим абонентам сети (рис. 7.2). Процесс «подписания» сообщения происходит следующим образом. информации

бранного алгоритма ЭЦП шифрует передаваемую информацию, представленную в цифровом виде, или производную от этого сообщения, полученную путем сжатия информации в соответствии с определенными математическими преобразованиями (хеш-функцией). Полученная таким образом шифрованная последовательность и есть цифровая подпись. Далее отправитель информации по открытому каналу связи посылает незашифрованную информацию и

- Полученную получатель сообщения
- Алгоритм

- ЭЦП
- Отправитель сообщения
- Передаваемое сообщение
- Канал связи
- Хеш-функция
- Алгоритм ЭЦП
- Секретный ключ
- тг
- Открытый ключ
- Открытый Проверка ключ ЭЦП Информация о принадлежности открытого ключа
- Удостоверяющий центр

Рис. 5.1. Алгоритм формирования ЭЦП

Получатель сообщения с помощью открытого ключа и выбранного алгоритма ЭЦП расшифровывает цифровую подпись. Далее он сравнивает принятую незашифрованную информацию и информацию, полученную при расшифровании цифровой подписи. Если цифровая подпись не была подделана и передаваемая открытая информация не искажена, то их тексты должны полностью совпасть. Если подпись подделана, то принятая открытая информация и информация, полученная при расшифровании,

будут различаться.

Если пользователь ведет переписку с несколькими абонентами сети и использует открытые ключи ЭЦП, то он должен безошибочно определять, какой из открытых ключей какому пользователю принадлежит. В случае ошибок на этом этапе функционирования ЭЦП возможно неправильное определение источника сообщения со всеми вытекающими отсюда по- следствиями. Важно, чтобы информация о принадлежности открытого ключа определенному пользователю была документально оформлена, и >то оформление должно быть выполнено специально назначенным ответственным органом.

Сертификат подписи. Документ, удостоверяющий подпись, получил название сертификата открытого ключа ЭЦП (сертификат подписи). Он подтверждает принадлежность открытого ключа ЭЦП владельцу секретного ключа подписи. Такой документ должен выдаваться удостоверяющим центром открытых ключей подписи.

Наличие такого документа важно при разрешении споров о создании того или иного документа конкретным лицом. Чтобы исключить возможность внесения изменений в сертификаты ключей со стороны пользователей при передаче их по каналам связи, сертификат в виде электронных данных подписывается ЭЦП удостоверяющего центра.

Таким образом, удостоверяющий центр выполняет функции электронного нотариуса и подтверждает легитимность подписанного электронного документа. Поэтому такой нотариус, как и обычный государственный нотариус, должен исполнять свои функции на основании лицензии, выданной государственным органом.

Как было сказано выше, для узаконивания рассмотренных механизмов использования ЭЦП был принят Федеральный закон «Об электронной цифровой подписи». В законе уточнены некоторые понятия, определяющие основные принципы пользования электронными документами. Так, под ЭЦП понимается «реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе». При этом владельцем сертификата ключа подписи является «физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы)».

Важным является определение факта подтверждения подлинности ЭЦП в электронном документе - как «положительного результата проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сер- тификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе».

Законом определены условия признания равнозначности электронной цифровой подписи и собственноручной подписи (ст. 4). ЭЦП в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при

одновременном соблюдении следующих условий: •

сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания; •

подтверждена подлинность ЭЦП в электронном документе; •

ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Поскольку основным документом, подтверждающим подлинность ЭЦП и идентификацию владельца, является сертификат ключа подписи, в законе достаточно подробно определены сведения, которые он содержит, а также сроки и порядок его хранения в удостоверяющем центре.

Отдельно рассмотрена деятельность удостоверяющих центров, их статус и взаимоотношения между этими центрами и владельцами сертификатов ключа подписи.

В заключение необходимо отметить важность узаконивания техни- ко-математических решений, применяемых при использовании ЭЦП. Это вызвано тем, что в настоящее время существует множество алгоритмов шифрования информации, ЭЦП, способов их программной реализации. В математике также существует довольно большой набор различных функций хеширования. Чтобы обеспечить возможность обмена информацией между абонентами, необходимо закрепление единого алгоритма ЭЦП и функции хеширования, достаточно полно удовлетворяющих требованиям безопасности и достоверности информации. В наиболее развитых странах существует практика задания алгоритма ЭЦП и функции хеширования в виде государственных стандартов. Такие стандарты существуют и в РФ. Первым отечественным стандартом ЭЦП является принятый в 1994 г. и действующий в настоящее время ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

В целях повышения криптографических качеств ЭЦП, гарантирующих при сохранении в тайне закрытого ключа подписи невозможность её подделки в течение нескольких десятков лет даже с учётом развития вычислительной техники и соответствующих математических алгоритмов, с 2000 г. специалисты ФАПСИ

начали разработку нового стандарта. Постановлением Госстандарта России № 380-СТ от 12 сентября 2001 г. разработанный ФАПСИ проект стандарта ЭЦП утвержден в качестве государственного стандарта ГОСТ Р34.10-2001 и введен в действие с 1 июля 2002 г.

Таким образом, в РФ в настоящее время имеется благоприятная возможность получить взаимоувязанное решение как юридических и организационных вопросов, связанных с применением ЭЦП в документообороте, гак и технических вопросов, и вопросов качества, связанных с криптографическими свойствами процедур ЭЦП.

В соответствии с «Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» средства ЭЦП относятся к криптографическим. Порядок их разработки и использования будет рассмотрен ниже.

6. Законодательство в сфере защиты информации.

Одной из наиболее сложных проблем, в определенной мере, сдерживающей темпы информатизации общества, является необходимость приоритетного обеспечения вопросов национальной безопасности (социальной, экономической, политической и т.д.) в условиях широкого применения средств вычислительной техники и связи для обработки конфиденциальной и биржевой инфраструктурах. Социально-экономические последствия широкого внедрения компьютеров в жизнь современного общества привели к появлению ряда проблем информационной безопасности.

В связи с возрастающим числом компьютерных преступлений проблема защиты информации является приоритетной в настоящих условиях. Защита информации должна носить комплексный характер.

Комплексный характер защиты достигается за счет использования унифицированного алгоритмического обеспечения для средств криптографической защиты в соответствии с российскими государственными стандартами:

ГОСТ 28147-89

Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

ГОСТ Р 34.10-94

Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

ГОСТ Р 34.11-94

Информационная технология. Криптографическая защита информации. Функция хэширования.

ГОСТ Р 50739-95

Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

Алгоритмы реализованы в виде единого комплекса средств криптографической защиты информации (СКЗИ), сертифицированных ФАПСИ, а также единых ключевых систем.

Свою деятельность ЗАО МО ПНИЭИ строит в соответствии с законодательством РФ в области криптографической защиты информации.

6.1. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также

ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

(п. 7 введен Федеральным законом от 21.07.2014 N 242-ФЗ)

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты

должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

7. Ключи электронной подписи

7.1. Что представляют собой ключи ЭЦП

Электронно-цифровая подпись — это информация в электронной форме (п. 1 ст. 2 закона «Об электронной подписи» от 06.04.2011 № 63-ФЗ), которая может дополнять тот или иной файл в целях удостоверения его авторства, а также подтверждения факта отсутствия изменений в данном файле после его подписания. Программная оболочка, посредством которой генерируется соответствующая информация, формирует электронный ключ.

При этом данный ключ классифицируется на 2 разновидности:

- открытый;
- закрытый.

Изучим их специфику.

7.2. Открытый ключ

Под открытым ключом ЭЦП понимается уникальная последовательность символов (п. 5 ст. 2 закона № 63-ФЗ), которая доступна всем пользователям, желающим проверить подписанный с помощью ЭЦП документ на предмет авторства и целостности. Обычно открытый ключ находится в распоряжении получателя файлов, подписанных ЭЦП.

7.3. Закрытый ключ ЭЦП

Под закрытым **ключом электронной подписи** понимается, в свою очередь, последовательность символов, посредством которых осуществляется непосредственно подписание файла и удостоверение его авторства и целостности (п. 6 ст. 2 закона № 63-ФЗ). Доступ к закрытому ключу имеет только автор файла (или уполномоченное на работу с данным файлом лицо).

Открытые и закрытые **ключи электронной подписи** связаны между собой: проверить корректность ЭЦП, сформированной с помощью закрытого ключа, можно только с помощью соответствующего ему открытого ключа. То есть у них должен быть общий производитель (таковым может быть удостоверяющий центр).

Что представляет собой носитель ключа электронной подписи:

Открытый и закрытый ключи создаются с помощью специальных криптографических приложений. Располагаются они на особом носителе — хорошо защищенном от несанкционированного копирования данных аппаратном модуле (например, устройстве типа eToken). Пользоваться им может только человек, имеющий правомочия в части подписания тех или иных файлов.

8. Основные сведения

Центр сертификации — это компонент, отвечающий за управление криптографическими ключами пользователей.

Открытые ключи и другая информация о пользователях хранится центрами сертификации в виде цифровых сертификатов, имеющих следующую структуру:

- серийный номер сертификата;
- объектный идентификатор алгоритма электронной подписи;
- имя удостоверяющего центра;
- срок действия сертификата;
- имя владельца сертификата (имя пользователя, которому принадлежит сертификат);
- открытые ключи владельца сертификата (ключей может быть несколько);
- объектные идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;
- электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра (подписывается результат хеширования всей

информации, хранящейся в сертификате).

Отличием аккредитованного центра является то, что он находится в договорных отношениях с вышестоящим удостоверяющим центром и не является первым владельцем самоподписанного сертификата в списке удостоверенных корневых сертификатов. Корневой сертификат аккредитованного центра удостоверен вышестоящим удостоверяющим центром в иерархии системы удостоверения. Таким образом, аккредитованный центр получает «техническое право» работы и наследует «доверие» от организации, выполнившей аккредитацию.

Аккредитованный центр сертификации ключей обязан выполнять все обязательства и требования, установленные законодательством страны нахождения или организацией, проводящей аккредитацию в своих интересах и в соответствии со своими правилами.

Порядок аккредитации и требования, которым должен отвечать аккредитованный центр сертификации ключей, устанавливаются соответствующим уполномоченным органом государства или организации, выполняющей аккредитацию.

Центр сертификации ключей имеет право:

- предоставлять услуги по удостоверению сертификатов электронной цифровой подписи
- обслуживать сертификаты открытых ключей
- получать и проверять информацию, необходимую для создания соответствия между информацией, указанной в сертификате ключа, и предъявленными документами.

9. Носители ключей электронной подписи

Что такое носитель электронной подписи? Теоретически – это любой накопитель, на который записаны метаданные ЭЦП в зашифрованном виде. С целью защиты персональных данных для этого сейчас используются:

9.1. Варианты носителей ЭП И ЭЦП

Наиболее безопасный носитель ключа – eToken и ruToken, в дальнейшем для этого можно будет также использовать SIM-карту. Современные носители обладают

следующими особенностями:

- eToken – это защитное устройство, позволяющее обеспечивать полную сохранность цифровых ключей, сертификатов и прочей важной информации. Он представляет собой смарт-карту или USB-ключ и может использоваться со всеми приложениями, работающими в сфере Public Key Infrastructure. Подключение такого носителя ключа электронной подписи к компьютеру позволяет работать с ЭЦП и цифровыми сертификатами. Такие ключи одобрены ФСБ и ФСТЭК, они соответствуют требованиям законодательства.
- ruToken – идентификатор небольшого размера, выполненный в виде USB-брелка. Такое устройство позволит больше не запоминать сложные пароли: они записываются в память и используются при необходимости. Носитель ключа электронной подписи для Госусулг и других сайтов государственных органов достаточно подключить к компьютеру через USB-разъем, после этого вводится PIN-код. Максимальный объем энергонезависимой памяти устройства составляет 128 Кб. В корпус встроен микроконтроллер, отвечающий за хранение и криптографическое преобразование зашифрованной информации.
- JaCarta LT – USB-токен со встроенным чипом. Он обеспечивает более высокий уровень безопасности и не требует установки дополнительного программного обеспечения.
- Использование РуТокена соответствует стандарту шифрования ГОСТ 28147-89, поэтому он получил наибольшее распространение. С его помощью удобно хранить зашифрованные ключи и сложные цифровые пароли, состоящие из множества символов.

Ключи и электронные сертификаты могут записываться на обычные флеш-накопители, однако в этом случае трудно обеспечить безопасность информации. Хищение флешки приведет к краже подписи, и злоумышленник сможет легко использовать ее в противоправных целях. Однако в ближайшем будущем граждане смогут пользоваться вместо РуТокена обычной Сим-картой. Это позволит значительно упростить и ускорить подписание документов в электронной форме.

Носитель ключа ЭП обязательно защищается индивидуальным паролем, который знает только владелец ЭП:

Считать информацию с такого накопителя может любое устройство, однако она будет представлена в шифрованном виде с применением криптографических алгоритмов (текущий принятый стандарт ГОСТ 28147-89).

Самым распространенным на текущий момент носителем для электронной подписи являются именно USB-токены ввиду своей невысокой стоимости. При этом они надежны, работать с ними можно на любом компьютере при наличии USB-порта (а для смарт-карт, к примеру, необходимо приобретать дополнительное считывающее устройство).

На рутокены записывается не только данные электронной подписи, но и специальное ПО для расшифровки данных. Общий объем встроенной энергонезависимой памяти в них составляет всего 128 килобайт. Для взаимодействия с ними необходимо устанавливать специализированное ПО и драйвера (поставляются в комплекте с устройством).

10. Процедура проверки электронной подписи.

Есть несколько методик проверки подлинности цифровой подписи. Самыми простыми из них являются проверка онлайн, на портале Госуслуг и с помощью специального программного обеспечения (например, программы «КриптоПро» и аналогичных). Но для продвинутых пользователей есть более сложные методы верификации средствами комплекса Microsoft Word или по значениям хеш-функций. Однако они больше подходят профессионалам, требуют специализированных утилит и глубоких познаний.

Цифровые технологии оказали серьёзное воздействие на жизненный уклад, в том числе на привычные алгоритмы ведения бизнеса: совершение платежей, оформление документов. Одна из самых серьёзных инноваций — электронная цифровая подпись (ЭЦП), прочно занявшая нишу системы обмена информацией, ряда банковских операций.

ЭЦП позволяет: подписать, подтвердить подлинность цифрового документа, установить его авторство. По сути это крипто-графически преобразованные сведения, эквивалент индивидуальной подписи, которые могут существенно усилить устойчивость электронного документа к взлому и подделке.

Функция хеширования

Хеш-функция или функция свёртки — функция, осуществляющая преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым

алгоритмом. Преобразование, производимое хеш-функцией, называется хешированием. Исходные данные называются входным массивом, «ключом» или «сообщением». Результат преобразования (выходные данные) называется «хешем», «хеш-кодом», «хеш-суммой», «сводкой сообщения».

Хеш-функции применяются в следующих случаях:

- при построении ассоциативных массивов;
- при поиске дубликатов в сериях наборов данных;
- при построении уникальных идентификаторов для наборов данных;
- при вычислении контрольных сумм от данных (сигнала) для последующего обнаружения в них ошибок (возникших случайно или внесённых намеренно), возникающих при хранении и/или передаче данных;
- при сохранении паролей *в системах защиты* в виде хеш-кода (для восстановления пароля по хеш-коду требуется функция, являющаяся обратной по отношению к использованной хеш-функции);
- при выработке электронной подписи (на практике часто подписывается не само сообщение, а его «хеш-образ»);
- и др.

В общем случае (согласно принципу Дирихле) нет однозначного соответствия между хеш-кодом (выходными данными) и исходными (входными) данными. Возвращаемые хеш-функцией значения (выходные данные) менее разнообразны, чем значения входного массива (входные данные). Случай, при котором хеш-функция преобразует более чем один массив входных данных в одинаковые сводки, называется «коллизией». Вероятность возникновения коллизий используется для оценки качества хеш-функций.

Существует множество алгоритмов хеширования, отличающихся различными свойствами. Примеры свойств:

- разрядность;
- вычислительная сложность;
- криптостойкость.

Выбор той или иной хеш-функции определяется спецификой решаемой задачи. Простейшим примером хеш-функции может служить «обрамление» данных циклическим избыточным кодом.

11. Применение хеш-функций

Хеш-функции широко используются в криптографии.

Хеш используется как ключ во многих структурах данных — хеш-таблицах, фильтрах Блума и декартовых деревьях.

Криптографические хеш-функции

Среди множества существующих хеш-функций принято выделять криптографически стойкие, применяемые в криптографии, так как на них накладываются дополнительные требования. Для того, чтобы хеш-функция {\displaystyle H} считалась криптографически стойкой, она должна удовлетворять трём основным требованиям, на которых основано большинство применений хеш-функций в криптографии:

- необратимость: для заданного значения хеш-функции m должно быть вычислительно неосуществимо найти блок данных X {\displaystyle X}, для которого $H(X)=m$ {\displaystyle H(X)=m};
- стойкость к коллизиям первого рода: для заданного сообщения M должно быть вычислительно неосуществимо подобрать другое сообщение N, для которого {\displaystyle H(N)=H(M)}$H(N)=M(N)$;
- стойкость к коллизиям второго рода: должно быть вычислительно неосуществимо подобрать пару сообщений {\displaystyle (M,M')}(M,M'), имеющих одинаковый хеш.

Данные требования не являются независимыми:

- обратимая функция нестойка к коллизиям первого и второго рода;
- функция, нестойкая к коллизиям первого рода, нестойка к коллизиям второго рода; обратное неверно.

Следует отметить, что не доказано существование необратимых хеш-функций, для которых вычисление какого-либо прообраза заданного значения хеш-функции теоретически невозможно. Обычно нахождение обратного значения является лишь вычислительно сложной задачей.

Для криптографических хеш-функций также важно, чтобы при малейшем изменении аргумента значение функции сильно изменялось (лавинный эффект). В частности, значение хеша не должно давать утечки информации даже об

отдельных битахаргумента. Это требование является залогом криптостойкости алгоритмов хеширования, хеширующих пользовательский пароль для получения ключа.

Хеширование часто используется в алгоритмах электронно-цифровой подписи, где шифруется не само сообщение, а его хеш-код, что уменьшает время вычисления, а также повышает криптостойкость. Также в большинстве случаев вместо паролей хранятся значения их хеш-кодов.

Контрольные суммы

Алгоритмы вычисления контрольных сумм — несложные, быстрые и легко реализуемые аппаратно алгоритмы, используемые для защиты данных от непреднамеренных искажений, в том числе — от ошибок аппаратуры. С точки зрения математики такие алгоритмы являются хеш-функциями, вычисляющими контрольный код. Контрольный код применяется для обнаружения ошибок, которые могут возникнуть при передаче и хранении информации.

Алгоритмы вычисления контрольных сумм по скорости вычисления в десятки и сотни раз быстрее, чем криптографические хеш-функции, и значительно проще в аппаратном исполнении.

Платой за столь высокую скорость является отсутствие криптостойкости — возможность легко «подогнать» сообщение под заранее известную контрольную сумму. Также обычно разрядность контрольных сумм (типичное число: 32 бита) ниже, чем разрядность криптографических хешей (типичные числа: 128, 160 и 256 бит), что означает возможность возникновения непреднамеренных коллизий.

Простейшим алгоритмом вычисления контрольной суммы является деление сообщения (входных данных) на 32- или 16-битовые слова с последующим суммированием слов. Такой алгоритм применяется, например, в протоколах TCP/IP.

Как правило, алгоритмы вычисления контрольных сумм должны обнаруживать типичные аппаратные ошибки, например, должны обнаруживать несколько подряд идущих ошибочных бит до заданной длины. Семейство алгоритмов так называемых «циклических избыточных кодов» удовлетворяет этим требованиям. К ним относится, например, алгоритм CRC32, применяемый в устройствах Ethernet и в формате сжатия данных ZIP.

Контрольная сумма, например, может быть передана по каналу связи вместе с основным текстом (данными). На приёмном конце, контрольная сумма может быть рассчитана заново и может сравниваться с переданным значением. Если будет обнаружено расхождение, то при передаче возникли искажения, и можно запросить повторную передачу.

Пример применения хеширования в быту — подсчёт количества чемоданов, перевозимых в багаже. Для проверки сохранности чемоданов не требуется проверять сохранность каждого чемодана, достаточно посчитать количество чемоданов при погрузке и выгрузке. Совпадение чисел будет означать, что ни один чемодан не потерян. То есть, число чемоданов является хеш-кодом.

Данный метод можно дополнить для защиты передаваемой информации от фальсификации (метод MAC). В этом случае хеширование производится криптостойкой функцией над сообщением, объединённым с секретным ключом, известным только отправителю и получателю сообщения. Криптоаналитик, перехватив сообщение и значение хеш-функции, не сможет восстановить код, то есть не сможет подделать сообщение (см. имитозащита).

12. Конфиденциальное делопроизводство

Конфиденциальное делопроизводство - это деятельность, обеспечивающая не только документирование и организацию работы с конфиденциальными документами, но и защиту от несанкционированного доступа и использования.

Словосочетание «конфиденциальный документ» является производным от понятия «документ». Образно выражаясь, если документ - это какое-то блюдо, то конфиденциальный документ - это блюдо, приправленное специями.

Согласно ГОСТ Р 51141 - 98, документом (документированной информацией) называется зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. Определение документированной информации содержится так же в ст. 2 Федерального закона от 27 июля 2006 г. №149 - ФЗ «Об информации, информационных технологиях и о защите информации»: «Документированная информация - зафиксированная на материальном носителе путем документирования информации с реквизитами, позволяющими определить такую информацию ли в установленных законодательством Российской Федерации случаях ее материальный носитель».

Основываясь на определениях термина «документ (документированная информация)», приведенных выше, можно предложить следующую формулировку понятия «конфиденциальный документ». Конфиденциальный документ (конфиденциальная документированная информация) - это зафиксированная на материальном носителе конфиденциальная информация с реквизитами, позволяющими ее идентифицировать.

Слово «идентифицировать» происходит от латинского identifico (отождествляю) и означает признать тождественность, отождествить объекты, опознать по определенным признакам. Свойство идентификации документированной информации придается реквизитам.

Реквизиты (от лат. Requisitum - необходимое) - это обязательные элементы оформления официальных документов, т.е. обязательные сведения, которые должны содержаться в документе для признания его действительным. Такими сведениями, как правило, являются название и адрес организации, составившей документ, регистрационный номер и дата регистрации документа, подписи ответственных лиц. Требования к бланкам документов, состав реквизитов документов и требования ких оформлению определяются стандартами на различные системы документации, например, ГОСТ Р 6.30 - 2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов». Отсутствие одного или нескольких реквизитов влечет за собой недействительность документа.

Среди реквизитов, позволяющих идентифицировать конфиденциальную информацию, необходимо в первую очередь отметить гриф конфиденциальности (реквизит, свидетельствующий о конфиденциальности информации, содержащейся в документе, проставляемый на самом документе и в сопроводительной документации к нему).

13. Защищенный электронный документооборот.

13.1. Электронный документооборот

Электронный документооборот — это система процессов по обработке документов в электронном виде. Большинство современных бухгалтерских и кадровых

программ умеют формировать электронные документы в стандартном установленном на законодательном уровне формате. Но чтобы такой документ обладал юридическим весом, он должен быть подписан обеими сторонами электронной подписью.

Электронный документооборот можно разделить на два больших вида — обмен документами внутри фирмы либо между разными компаниями по каналам связи. Допускается объединить эти две системы в одну глобальную.

13.2. КриптоСвязь

Юридически значимый документооборот — это документооборот, при котором участники системы совершают действия по принятию к исполнению документов в электронной форме, удостоверенных электронной подписью, и при этом несут ответственность за совершение, либо не совершение этих действий. Электронная подпись обеспечивает необходимую целостность, достоверность, аутентичность, неотказуемость и юридическую значимость электронных документов при соблюдении условий Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Группа компаний «Ижинформпроект» предлагает комплекс услуг по созданию и обслуживанию автоматизированных рабочих мест для обеспечения обмена конфиденциальными электронными юридически значимыми документами.

О системе

КриптоСвязь {Защищенный Электронный Документооборот} обеспечивает конфиденциальность, целостность, достоверность, аутентичность, неотказуемость и юридическую значимость передаваемых через систему электронных документов. Уровень применяемых средств защиты информации и организационных мероприятий в системе позволяет обмениваться электронными документами, содержащими конфиденциальную информацию (персональные данные, служебная, банковская, коммерческая тайна и т.п.).

Защищенный электронный документооборот реализуется с использованием базовых приложений Инфраструктуры открытых ключей (ИОК) / Public Key Infrastructure (PKI) — технологической инфраструктуры и сервисов, гарантирующих безопасность информационных и коммуникационных систем, использующих

криптографические алгоритмы с открытыми ключами.

При построении защищенного электронного документооборота применяются квалифицированная электронная подпись (а также шифрование) электронных документов, представленных в виде файлов, передаваемых между Участниами Системы, и квалифицированная электронная подпись и шифрование почтовых сообщений Internet. Для защиты электронных документов/сообщений используются сертифицированные средства криптографической защиты информации (СКЗИ) «КриптоПро CSP», а также совместимые с ними.

Функции системы

Применение сертифицированных СКЗИ обеспечивает использование в системе российских криптографических алгоритмов:

- Алгоритм зашифрования/расшифрования данных и вычисление имитовставки в соответствии с ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая»;
- Алгоритм формирования и проверки ЭЦП в соответствии с ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
- Алгоритм выработки значения хэш-функции в соответствии с ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Требования к пользователю

Для возможности работы в системе пользователь должен получить квалифицированный сертификат в Удостоверяющем центре InfoTrust ООО НПП «Ижинформпроект» в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». Сертификат содержит сведения о приложениях, системах документооборота, видах электронных документов, в которых разрешается его использовать.

Участники Системы руководствуются Регламентом системы КриптоСвязь{Защищенный Электронный Документооборот} , который устанавливает общий порядок взаимодействия Участников Системы с использованием средств защиты информации.

Регламент не устанавливает требований к форматам электронных документов, периодичности обмена, внутреннего учета и обеспечения защиты документов у Участников Системы. Участники Системы при необходимости устанавливают особые (дополнительные) условия взаимодействия.

14. Использование электронной подписи в договорном процессе.

Порядок заключения такого вида деловых документов, как договоры, регламентируется статьями из Гражданского и Трудового Кодексов:

- Статья 434 Гражданского Кодекса подтверждает, что договор между хозяйствующими субъектами (юридическими лицами, физическими лицами или некоммерческими организациями, ведущими от своего имени экономическую деятельность) можно заключить путем обмена электронными документами. Главное, чтобы можно было установить, что электронный документ исходит от стороны по договору.
- Статьи 312.1 и 312.2 Трудового Кодекса предусматривают, что договор с дистанционным сотрудником можно оформить в электронной форме.

В цифровом пространстве гарантом неизменности документа и подтверждения авторства выступает усиленная электронная подпись: квалифицированная или неквалифицированная. Применение электронной подписи в России регулируется федеральным законом № 63-ФЗ «Об электронной подписи» от 06.04.2011. Подробнее о видах электронной подписи можно прочитать в этой статье.

15. Социальные сети, движение и защита контента

15.1. Социальная сеть

Социальная сеть — онлайн-платформа, которую люди используют для общения, создания социальных отношений с другими людьми, которые имеют схожие интересы или офлайн-связи.

Подвиды

Помимо перечисленных социальных сетей имеются следующие типы ресурсов в формате Веб 2.0:

- Социальные закладки. Некоторые веб-сайты позволяют пользователям предоставлять в распоряжение других список закладок или популярных веб-сайтов. Такие сайты также могут использоваться для поиска пользователей с общими интересами. Пример: Delicious.
- Социальные каталоги напоминают социальные закладки, но ориентированы на использование в академической сфере, позволяя пользователям работать с базами данных цитат из научных статей. Примеры: Academic Search Premier, LexisNexis, Academic University, CiteULike, Connotea.
- Социальные библиотеки представляют собой приложения, позволяющие посетителям оставлять ссылки на их коллекции, книги, аудиозаписи и т. п., доступные другим. Предусмотрена поддержка системы рекомендаций, рейтингов и т. п. Примеры: discogs.com, IMDb.com.
- Социальные медиа-хранилища — сервисы для совместного хранения медиа-файлов. Их можно классифицировать по типу файлов, размещаемых на этих серверах.
- Специализированные социальные сети. Объединяют людей по определённым критериям (например, возраст, пол, вероисповедание, определённые увлечения и т. д.).
- Профессиональные социальные сети создаются для общения на профессиональные темы, обмена опытом и информацией, поиска и предложения вакансий, развития деловых связей. Примеры: LinkedIn, Мой Круг, Профессионалы.ру.
- Корпоративные социальные сети решают задачи организации и сопровождения деятельности компании.
- Сервисы для совместной работы с документами.
- Геосоциальные сети позволяют налаживать социальные связи на основании географического положения пользователя. При этом используются различные инструменты геолокации (например, GPS или гибридные системы типа технологии AlterGeo), которые дают возможность определять текущее местонахождение того или иного пользователя и соотносить его позицию в пространстве с расположением различных мест и людей вокруг.

15.2. Защита контента

Защита контента — методы защиты контента от копирования. Устанавливают скрипты, вставляющие ссылки в конце скопированного текста – так удалить эту ссылку дела нескольких секунд. Устанавливают плагины, которые блокируют выделение и копирование текста – так это примитивная защита контента, является препятствием только для новичков, которые если и копируют, то не с целью воровства, а с целью скопировать слово, ссылку, код.

Защита контента

- Правильно не бороться с растаскиванием контента, а использовать его себе на пользу
- Реализуем функционал защиты с помощью JavaScript – добавляем в буфер обмена ссылку на сайт при любом копировании материалов с сайта
- Добавляем сайт в сервис Яндекс.Вебмастер, добавляем ВСЕ статьи в «Оригинальные тексты» Подключаем авторство профиля Гугл+

15.3. Датчик движения

Датчик движения — сигнализатор, фиксирующий перемещение объектов и используемый для контроля за окружающей обстановкой или автоматического запуска требуемых действий в ответ на перемещение объектов.

Детектор движения — устройство или функция охранной телевизионной системы, формирующие сигнал извещения о тревоге при обнаружении движения в поле зрения видеокамеры.

Более чувствительную разновидность датчика движения называют также датчиком присутствия.

Литература

1. https://ru.wikipedia.org/wiki/

2. https://www.regberry.ru/malyy-biznes/elektronnaya-podpis

3. https://kontur.ru/diadoc/spravka/273-kep_edo

4.http://www.consultant.ru/document/cons_doc_LAW_112701/fd3323ec5de5f23f2340d6cab5ed9

5. https://lawbook.online/prava-pravovedenie-osnovyi/pravovyie-aspektyi-primeneniya-elektronnoy-20798.html

6. https://security.ru/legislation.php

7. https://nalog-nalog.ru/spravochnaya_informaciya/chto_takoe_i_kak_poluchit_klyuch_elektronnoj_podpisi/

8. https://ru.wikipedia.org/wiki/

9. https://pro-ecp.ru/etsp/stati/chto-takoe-i-kak-poluchit-nositel-klyucha-elektronnoj-podpisi.html

10. https://ca.kontur.ru/articles/proverka-elektronnoi-podpisi

11. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2002. — ISBN 5-89392-055-4.

https://ru.wikipedia.org/wiki/

12. https://www.bibliofond.ru/view.aspx?id=723046

13. https://www.infotrust.ru/cryptocon/protected-electronic-document

14. https://ca.kontur.ru/articles/kak-zaklyuchit-dogovor-v-elektronnoj-forme

15. https://ru.wikipedia.org/wiki/