

Рябошанка Тамара Владимировна

преподаватель специальных дисциплин

ГБПОУ Краснодарского края «Краснодарский колледж

электронного приборостроения»

г. Краснодар, Краснодарский край

**СОВРЕМЕННАЯ АКТИВНАЯ ФОРМА ПОВЫШЕНИЯ
КВАЛИФИКАЦИИ ПРЕПОДАВАТЕЛЯ КОЛЛЕДЖА НА ПРИМЕРЕ
ПРОВЕДЕНИЯ МАСТЕР-КЛАССА**

Аннотация: в представленной статье рассматривается вопрос применения мастер-класса как активной формы повышения квалификации на примере проведения занятия по дисциплине «Информационная безопасность».

Ключевые слова: мастер-класс, электронная цифровая подпись, педагогическое мастерство, получение сертификата.

На современном этапе развития России трудно переоценить значение образования, степень его влияния на всех участников образовательного процесса, поскольку треть населения России учится, учит, повышает квалификацию, проходит переподготовку.

В системе Российского образования идут сложные и противоречивые процессы: глубокое реформирование и развитие содержания образования с одной стороны, отставание по таким важнейшим направлениям как материально-техническое, финансово-экономическое и кадровое обеспечение с другой.

Актуальным становится выявление, обобщение и распространение инновационного педагогического опыта. Одной из эффективных форм распространения собственного педагогического опыта является такая современная форма методической работы как мастер-класс.

Педагогам необходимо постоянно учиться, чаще всего в условиях непрерывного образования и совершенствования своей профессиональной компетентности. Эффективным способом может стать взаимообмен профессиональным

опытом, взаимообучение, взаимосовершенствование своей педагогической деятельности. Оптимальной формой обучения и развития современных педагогов можно считать мастер-класс, причем независимо от общеобразовательной системы или системы профессионального образования. В процессе поиска путей повышения эффективности обучения учащихся педагог выявляет и вырабатывает новые формы, методы, приемы и средства педагогической деятельности.

Мастер-класс позволяет организовать обмен творческим опытом и повышение квалификации наиболее активных молодых преподавателей, обобщать и распространять педагогический опыт, представляющий собой фундаментально разработанный оригинальный метод или авторскую методику, опирающийся на свои принципы и имеющий определенную структуру.

Проведение мастер-класса, и особенно его подготовка – это кропотливый труд.

Во время мастер-класса ведущий специалист-мастер рассказывает и показывает, как применять на практике новую технологию или метод.

Целью мастер-класса является ретрансляция уникального педагогического опыта, в течение занятия научить и научиться чему-то конкретному.

Основные задачи мастер-класса.

- создание условий для профессионального общения, самореализации и стимулирования роста творческого потенциала учащихся;
- повышение профессионального мастерства и квалификации участников;
- внедрение новых технологий обучения и воспитания.

Основными преимуществами мастер-класса являются уникальное сочетание индивидуальной и коллективной работы, возможность приобретения и закрепления практических знаний и навыков, развития гибкости мышления.

Мастером могут быть предложены авторские методы применения технологий на практике, тонкости, нюансы и недокументированные возможности при использовании технологии в конкретных задачах.

Мастер должен создать атмосферу открытости, доброжелательности, творчества в общении. Его целью должна стать задача вовлечения участников

мастер-класса в процесс, разбудить в них то, что скрыто для них самих, устранить то, что мешает саморазвитию, передать способы деятельности.

Методика проведения мастер-классов не имеет единых норм, так как основывается на восприимчивости участников и на педагогической интуиции преподавателя, не имеет четкой структуры проведения.

Можно предложить мастер-класс по отработке практических навыков по технологии создания и применения Электронной цифровой подписи в государственных системах электронного документооборота и применение ее для ведения бизнеса на примере дисциплины Информационная безопасность специальности прикладная информатика.

Тема мастер-класса: «Создание и проверка электронной цифровой подписи (ЭЦП) средствами современных информационных компьютерных технологий (ИКТ)».

«Сегодня наиболее часто декларируется использование средств ИКТ для достижения следующих педагогических целей:

– развитие личности обучающихся, его подготовка к жизнедеятельности в условиях современного информационного общества с опорой на индивидуальность;

– реализацию социального заказа на подготовку специалистов, обладающих информационной компетентностью, формированию у них мировоззрения открытого информационного общества;

– повышению качества образовательного процесса» [4].

Цель занятия: изучить назначение и цели применения ЭЦП, нормативно-правовые документы по ЭЦП, изучить схему реализации и применения ЭЦП, получение сертификата ЭЦП, функции удостоверяющего центра, процедуру получения сертификата на базе Тестового Удостоверяющего Центра ООО «КРИПТО-ПРО». Это процесс моделирования реальных ситуаций получения ЭЦП. «В педагогической деятельности моделирование может рассматриваться в трех аспектах: как средство обучения, как инструмент познания и как объект изучения» [5].

Задачи занятия:

Образовательная: Развитие познавательных навыков в области применения криптографических методов защиты информации с использованием современных информационных технологий.

Развивающая: Развитие практического мышления, формирование умения применять полученные знания и навыки в области информационных технологий.

Воспитательная: Формирование общеучебных и общекультурных навыков работы с информацией. Формирование научного мировоззрения, культуры познания нового и применения полученных навыков и умений.

Требования к материальному обеспечению мастер-класса:

1. Персональные компьютеры (ПК) для каждого студента (компьютерный класс).
2. Презентация на каждом рабочем месте и на большом экране (Стене).
3. Стена (большой Экран).
4. Видеоролик об ЭЦП для бизнеса.
5. Тестовая оболочка «MyTest» с тестом по основным понятиям из ФЗ №63 доступна на всех ПК.
6. Доступ в Интернет на всех ПК.
7. Нормативно-справочная документация по ЭЦП.

Тип занятия – интегрированный (лекционно-практическое занятие): изучение основных понятий и определений, выполнение практического задания по алгоритму с использованием сервисов Интернет.

Алгоритм проведения мастер-класса:

Первый этап – Постановка проблемы или активизация проблемы. Актуальность знаний, навыков и умений по ЭЦП.

Мастер-класс проводится в хорошо оборудованном Информационном центре Краснодарского колледжа электронного приборостроения.

Участники мастер-класса удобно располагаются за ПК в Информационном центре колледжа.

Перед участниками и гостями расположен большой экран, на котором демонстрируется презентация, включающая тему, объяснения мастера, вопросы теста, результаты тестирования, экранные формы алгоритма получения Сертификата.

Мастер приветствует всех собравшихся в этом комфортном зале. Объявляет, что объектом нашего внимания на проводимом мастер-классе будет электронная цифровая подпись.

Далее мастер со студентами ведет диалог по ранее рассматриваемым на занятиях вопросам о необходимости использования электронной цифровой подписи, о ее применении в различных видах человеческой деятельности.

Подтверждением необходимости изучения и применения такого инструмента как электронная цифровая подпись является диаграмма выданных сертификатов ключей проверки ЭЦП.

Данные на сентябрь 2016 отражаются на диаграмме (рис. 1).



Рис. 1. Диаграмма выдачи сертификатов ключей проверки ЭЦП

Из диаграммы видно, что количество выданных сертификатов неуклонно растет. Развитие информационного сообщества в Российской Федерации стремительно набирает обороты: большинство бизнес-процессов различных предприятий происходит в электронной форме, граждане РФ используют Интернет

для получения необходимой информации, государственные органы исполнительной власти реализуют свои функции и оказывают услуги с помощью веб-решений.

Широкое внедрение информационных технологий в повседневную жизнь стало возможным благодаря применению электронной цифровой подписи. Определение ЭЦП в Российской Федерации было введено в 2002 году Федеральным законом «Об электронной цифровой подписи» №1-ФЗ от 10.01.2002 года. Федеральный закон наделил электронную цифровую подпись полномочиями заверять электронные документы и приравнял ЭЦП по юридической значимости к собственноручной рукописной подписи.

Появление такого инструмента как электронная цифровая подпись обусловило появление первых систем юридически-значимого электронного документооборота. Предприятия-налогоплательщики получили возможность сдавать отчетность (налоговые декларации, бухгалтерские балансы) в инспекции ФНС через интернет, заверив их ЭЦП. В банках большую популярность стали приобретать системы Банк-Клиент, с помощью которых различные организации и в настоящее время совершают электронные денежные переводы, при этом платежные поручения также подписываются электронной подписью.

В настоящее время предприятия ведут полноценный электронный юридически-значимый документооборот со всеми контролирующими органами – Федеральной налоговой службой, Пенсионным Фондом, Фондом социального страхования, Росстатом и т. д. Электронная цифровая подпись освободила всех участников финансовых операций от обязанности вести бумажный документооборот, тем самым у бизнеса появились новые возможности для развития партнерских взаимодействий в различных, даже самых удаленных регионах.

В основе создания использования ЭЦП лежат математические принципы. В России в 1994 г. были приняты государственными стандарты функций, образующих систему ЭЦП: ГОСТ 34.10–94, ГОСТ 34.11–94.

Стандарт ГОСТ 34.10–94 устанавливает процедуры выработки и проверки электронной цифровой подписи сообщений (документов), передаваемых по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения, на базе асимметричного криптографического алгоритма с применением функции хеширования.

Внедрение системы ЭЦП на базе настоящего стандарта обеспечивает защиту передаваемых сообщений от подделки, искажения и однозначно позволяет доказательно подтвердить подпись лица, подписавшего сообщение.

Система ЭЦП базируется на методах криптографической защиты данных с использованием хеш-функции. Алгоритмы вычисления функции хэширования установлен в ГОСТ Р 34.11–94.

Процедуры цифровой подписи допускают как программную, так и аппаратную реализацию. Система ЭЦП включает в себя процедуры выработки и проверки подписи под данным сообщением.

Система ЭЦП содержит три алгоритма (рис. 2):

1. Хеширования.
2. Выработки ЭЦП под документом.
3. Проверки подписи.

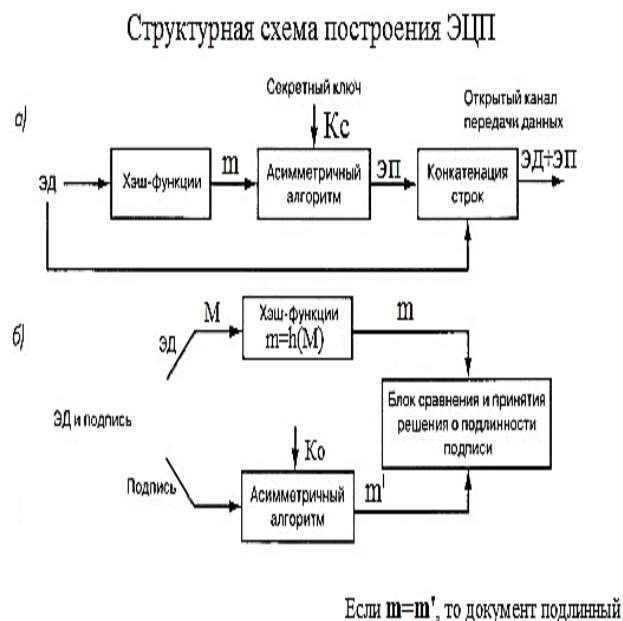


Рис. 2. Схема построения ЭЦП

Необходимость официального признания ЭЦП явилась результатом всевозрастающего потока электронных документов, а также появлением алгоритмов ЭЦП, обладающих высокой степенью защищенности (невозможности подделки).

Чтобы более детально разобраться с назначением электронной цифровой подписи, нужно рассмотреть ее назначение.

Электронная цифровая подпись позволяет выполнять функции:

1. Помогает минимизировать финансовые потери – это достигается благодаря тому, что степень конфиденциальности информации существенно возрастает.

2. Сокращает время движения документов между контрагентами – обмен документацией происходит в считанные минуты.

3. ЭЦП дает возможность подписывать отчетность, которая сдается в государственные органы по электронной почте.

4. Пользователь ЭЦП может участвовать в электронных торгах. Позволяет экономить денежные средства предприятия, так как процедура подготовки, доставки и учета различных документов становится менее затратной.

5. Обеспечивает эффективную работу с иностранными партнерами, ускоряя документооборот на международном уровне.

6. Благодаря ЭЦП временные границы в бизнесе стираются, а сделки заключаются моментально.

Таким образом, приобретая электронную цифровую подпись, предприниматель обеспечивает процветание своему бизнесу.

Второй этап – Презентация о роли электронной подписи в информационном сообществе.

Электронная цифровая подпись является наиболее оптимальным вариантом для тех предпринимателей, которые хотят идти в одну ногу со временем. Особую популярность ЭЦП набирает в условиях тех требований, которые диктует современный бизнес, для которого характерна глобализация. Если у Вас нет времени

на ожидание курьера с пакетом документов, то пора задумать о том, что нужно получить ЭЦП, и тем самым, избавиться от головной боли, связанной с доставкой почты.

Мастер на занятии объясняет преимущества ЭЦП, приводя пример из жизни: «Представьте, что Вы хотите заключить выгодный контракт на большую сумму с иностранным партнером. Чтобы обезопасить себя от того, что контрагента переманит на свою сторону конкурент, пока партнер будет ждать от Вас документов, договор можно подписать с помощью электронной подписи. При этом ЭЦП полностью подтверждает подлинность документа, так как она на юридическом уровне приравнивается к подписи директора и печати предприятия».

Таким образом, именно благодаря ЭЦП временные границы в бизнесе стираются, а сделки заключаются моментально.

Затем раскрывается вопрос о возможности подделки ЭЦП: «Этот вопрос волнует многих бизнесменов, которые решили приобрести ЭЦП для осуществления хозяйственной деятельности. Можно сказать то, что подделать электронную подпись практически невозможно, так как она создается путем применения огромного количества математических вычислений. Каждая электронная подпись подлежит обязательной сертификации в Удостоверяющем Центре открытого ключа подписи. Это говорит о том, что ЭЦП имеет высокий уровень защиты. При желании, можно даже застраховать ЭЦП в этом же центре. Чтобы пользоваться ЭЦП, осуществляя ежедневные хозяйственные операции, не нужны особые знания. Необходимо понимать, что пользователь получает открытый и закрытый криптографический ключ. Главная роль отводится именно секретному ключу, благодаря которому осуществляется шифрование электронного документа и формируется в итоге ЭЦП. Секретный ключ пользователь получает на отдельном носителе. Доступ к нему должны иметь только определенные работники. Чтобы подписать документ электронной подписью, нужно всего лишь установить под ним ЭЦП.

Электронный документооборот практически невозможен без применения электронной цифровой подписи.

Электронная цифровая подпись обеспечивает:

1. Подлинность – ЭЦП помогает гарантировать, что поставивший подпись – тот, кем он является в действительности.
2. Целостность – ЭЦП позволяет гарантировать, что содержимое документа не менялось и не подделывалось после ввода цифровой подписи.
3. Неотрекаемость – ЭЦП помогает доказать любой из сторон авторство подписанного содержимого.

Затем мастер акцентирует внимание слушателей на федеральных законах: «Активное проникновение электронной цифровой подписи в различные сферы информационного сообщества обусловило усиление законодательной базы и необходимость правового регулирования вопросов электронного взаимодействия, а также ответственность Удостоверяющих Центров. На смену Федеральному закону №1-ФЗ «Об электронной цифровой подписи» от 10.01.2002 года пришел Федеральный закон №63-ФЗ «Об электронной подписи» от 06.04.2011 года, который расширил и конкретизировал определение электронной подписи, а также установил ответственность Удостоверяющих Центров перед владельцами ЭЦП.

Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

Для целей настоящего Федерального закона используются следующие основные понятия: электронная подпись, сертификат ключа проверки электронной подписи, квалифицированный сертификат ключа проверки электронной подписи, владелец сертификата ключа проверки электронной подписи, ключ электронной подписи, ключ проверки электронной подписи, удостоверяющий центр, средства электронной подписи, участники электронного взаимодействия, информационная система общего пользования, подтверждение владения ключом электронной подписи».

Все понятия и определения показаны на слайдах презентации. Презентация доступна каждому слушателю.

Третий этап – Для контроля усвоения основных понятий и определений, связанных с ЭЦП, а также определения уровня подготовленности слушателей предлагается прохождение теста, реализованного в оболочке «MyTest».

Всем слушателям предлагается пройти контрольный тест по овладению знаниями в части ЭЦП, который установлен на каждом ПК. Результаты тестирования сохраняются в протоколе оболочки «MyTest» и выводятся на большой экран. Мастер может сделать выводы об уровне подготовленности аудитории и далее принимать решение о степени детализации применения нового материала.

Четвертый этап – практические действия мастера и участников – это создание сертификата средствами программного продукта Тестового Удостоверяющего Центра компании ООО «КРИПТО-ПРО».

Мастер дает необходимые определения:

«Удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей.

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном Федеральным законом порядке выдан сертификат ключа проверки электронной подписи. В процессе формирования электронного ключа, данные о его владельце сохраняются в отдельный файл. Этот файл и является сертификатом ключа подписи».

Нововведения в законодательной базе и переход на квалифицированную электронную подпись стали большим шагом вперед на пути к объединению разрозненных информационных систем. В соответствии с Федеральным законом №63-ФЗ «Об электронной подписи» информационные системы государственных органов исполнительной власти обязаны принимать усиленные квалифицированные сертификаты, выпущенные Удостоверяющими Центрами по единым требованиям. Вслед за государственными информационными системами, на использование квалифицированной электронной цифровой подписи переходят и коммерческие интернет ресурсы.

Таким образом, определение единых требований к электронной подписи стало первым важным шагом на пути к созданию единого унифицированного информационного пространства, в котором были бы четко определены формы и форматы документов, требования, роли, полномочия, ответственность – всех участников взаимодействия, в том числе и самих информационных систем.

В ходе мастер-класса участникам предлагается воспользоваться услугами Тестового Удостоверяющего Центра ООО «КРИПТО-ПРО» для получения сертификата. Необходимо выйти на сайт ООО «КРИПТО-ПРО». Найти закладку Тестовый Удостоверяющий Центр.

На странице появится инструкция и руководство для генерации сертификата.

Используя презентацию, мастер демонстрирует пошаговый алгоритм получения сертификата средствами Тестового Удостоверяющего Центра.

После комментариев мастера можно приступить к получению сертификата. Необходимо выполнить действия в трех закладках после заголовка «Получить сертификат» на странице Тестового Удостоверяющего Центра.

Центр предназначен только для целей тестирования и не должен использоваться для других целей.

Центр не проверяет информацию, указанную в запросах на сертификат. Не следует доверять сертификатам, выданным Тестовым Удостоверяющим Центром.

Пятый этап – рефлексия. В итоге мастер-класса и демонстрируемого приема участники и слушатели познакомятся с процессом создания сертификата и освоят алгоритм получения сертификата ключа проверки электронной цифровой подписи средствами Тестового Удостоверяющего Центра ООО «КРИПТО-ПРО». Приемы и методы, демонстрируемые в рамках мастер-класса, участники могут использовать на практике в реальных условиях.

Успешным результатом индивидуальной выполненной работы на своем рабочем месте является получение сертификата ключа проверки электронной подписи.

Мастер-класс – это активная форма творческой самореализации педагога, когда мастер передает свой опыт слушателям путем прямого и комментированного показа приемов своей работы, правильной организации работы, раскрывает творческий потенциал всех его участников.

Проведение мастер-класса и его подготовка является хорошей школой повышения профессионального мастерства педагога, раскрытию его личностного потенциала и роста мастерства.

Список литературы

1. Борисов М.А. Основы программно-аппаратной защиты информации / М.А. Борисов, И.В. Заводцев, И.В. Чижов. – М.: ЛЕНАРД, 2014. – 416 с.
2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты / А.А. Петров. – М.: ДМК, 2000. – 448 с.
3. Селевко Г.К. Альтернативные педагогические технологии. – М.: НИИ школьных технологий, 2005. – 224 с.
4. Фешина Е.В. О воспитательном потенциале средств ИКТ / Стандарты и мониторинг в образовании. – 2011. – №6. – С. 56–57.
5. Юнов С.В. Воспитательные возможности ролевого информационного моделирования // Вестник Российского университета дружбы народов. Серия: Информатизация образования. – 2011. – №2. – С. 60–63.

6. Федеральный закон от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи» Принят Государственной Думой 25 марта 2011 года. Одобрен Советом Федерации 30 марта 2011 года // Российская газета – Федеральный выпуск №5451 (75).

7. Государственный стандарт Российской Федерации ГОСТ Р 34.10–94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма». Введен 01.01.1995.

8. Государственный стандарт Российской Федерации ГОСТ Р 34.11–94 «Информационная технология. Криптографическая защита информации. Функция хэширования». Введен 01.01.1995.