

Отдельной строкой в проблеме обеспечения ИБ КИС как любой АС стоит оценка уровня ее ИБ. Согласно стандарту ГОСТ Р ИСО/МЭК ТО 19791 этот процесс состоит из следующих этапов: а) определение целей безопасности для АС, которые уменьшат неприемлемые риски до приемлемого уровня; б) выбор и спецификация технических и организационных мер безопасности, которые соответствуют целям безопасности АС, принимая во внимание уже реализованные меры обеспечения безопасности; в) определение конкретных измеримых требований доверия как к техническим, так и организационным мерам обеспечения безопасности, чтобы удостовериться в том, что АС соответствует целям безопасности; г) фиксирование принятых решений в задании по безопасности для АС (ЗБС); д) оценка конкретной АС с тем чтобы сделать вывод о ее соответствии ЗБС; е) периодическая переоценка рисков безопасности АС, так и способности АС противостоять этим рискам.

Выполнение всех обозначенных процессов будет проходить на модернизации КИС образовательного назначения. Все обозначенные положения выполнимы и для такого рода систем.

Список литературы

1. Назарова, О.Б. Сопровождение корпоративных информационных систем [Текст] : учебник / О.Б. Назарова, Л.З. Давлеткиреева, О.Е. Масленникова, Н.О. Пролозова. – Магнитогорск : МаГУ, 2013. – 220 с.
2. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью. [Электронный ресурс] – Режим доступа: http://www.rosintelcom.ru/upload/nonnormativnaja_basa_zakoni/GOST-17799-2005.pdf (дата обращения: 22.02.2014).
3. ГОСТ 34.601-90 Автоматизированные системы. Стадии создания [Электронный ресурс] – Режим доступа: http://www.ptj-exp.ru/gost/gost_34-601-90.php (дата обращения: 22.02.2014).
4. ГОСТ Р ИСО/МЭК ТО 19791 – 2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем [Электронный ресурс]. – Режим доступа: <http://standartgost.ru/> (дата обращения: 22.02.2014).

УДК 347.78:004.056

С.В. Ченушкина МЕТОДЫ БОРЬБЫ С ПЛАГИАТОМ И ЗАЩИТЫ АВТОРСКОГО ПРАВА

Ченушкина Светлана Владимировна

Svch2003@yandex.ru

ФГАОУ ВПО «Российский государственный профессионально-педагогический университет», Россия, г. Екатеринбург

METHODS OF DEALING WITH PLAGIARISM AND COPYRIGHT PROTECTION

Chenushkina Svetlana

Russian State Vocational Pedagogical University, Russia, Yekaterinburg

Аннотация . В статье рассматривается техническая сторона защиты авторских прав. Описываются основные способы и методы защиты от плагиата.

Abstract. The article considers the technical side of copyright protection. Describes the main ways and methods of protection against plagiarism.

Ключевые слова: авторское право, плагиат, интеллектуальная собственность.

Keywords: copyright, plagiarism of copyright, intellectual property.

Благодаря компьютерным технологиям качественное образование современному человеку доступно в электронном формате. Студент может обучаться в своем родном городе, даже если ближайший университет находится за границей. Критерии допуска ниже, чем для очно-заочного обучения, то есть допускаются все желающие. При этом нет необходимости постоянного обучения — достаточно сформировать свой собственный график согласно предложенной учебной программе, следовать ему и вовремя сдавать онлайн-сессию: не нужно отпрашиваться с работы или клянчить отпуск за свой счет на время сдачи экзаменов.

Сегодня в нашей стране заочное и дистанционное обучение проходят более 2 000 000 студентов. Значительное увеличение спроса на соответствующие услуги государственных и аккредитованных негосударственных вузов отмечено после экономического кризиса 2008-2009 годов.

По данным «Независимой газеты» к 2010 году уже более половины абитуриентов выбирали заочное образование. Есть сразу несколько причин такого выбора. Во-первых, более низкие цены на обучение. В среднем, студенты, получающие заочное или дистанционное образование, экономят 40-50% (а иногда даже до 70%). Кроме того, не требуется тратить значительные средства на проживание в другом городе и поездки на занятия и сессии.

Далеко не все отечественные вузы могут активно развивать дистанционные формы обучения. Причина — недостаточные технические ресурсы и нехватка профессорско-преподавательских кадров, имеющих возможность создавать авторские учебные курсы. Также необходимо создать единую систему контроля учебного процесса, гарантий его качества. И, самое главное, создать библиотеку курсов и программ обучения, каждая из которых является интеллектуальной собственностью и стоит десятки и даже сотни тысяч долларов.

Когда речь заходит об интеллектуальных работах, сразу возникает вопрос о защите авторских прав, в которой нуждаются и методисты, составляющие программы, и преподаватели, подготавливающие их содержание, и обучаемые, при написании дипломов и курсовых. И, конечно, программисты, которые компьютерным кодом связывают воедино все звенья цепи.

В данной статье мы попытаемся частично решить проблему защиты авторских прав, рассмотрев несколько подходов и мер предохранения от плагиата.

Сетевая технология является наиболее распространенной в системе электронного обучения, где необходимые учебные материалы размещаются в электронном виде на сайте центра или высылаются обучаемому по электронной почте. Но, говоря об Интернете, мы сталкиваемся с нерегулируемым и право незащищенным информационным сообществом. Интернет предоставляет доступ к огромному количеству информации, игнорируя ее стоимость, контроль над содержанием и защиту авторских прав. Если информация доступна в электронном варианте, ее практически невозможно контролировать, так как она может быть загружена, скопирована, утрачена, или напротив — сохранена, изменена или продана.

С одной стороны в случае полного копирования материала или с небольшими изменениями, плагиат будет виден явно, что упростит процедуру доказывания в суде. Но в случае заимствования учебных программ и планов и построение на их основе учебного процесса своего учебного заведения ситуация не так очевидна.

К примеру, в статье Н.Д. Кликунова приводится ситуация, в которой один вуз может паразитировать за счет другого, разработавшего и внедрившего систему дистанционного образования. В частности, использованием разработанных учебных программ или методических разработок, предоставляемых в электронном виде обучаемым [2].

Возникает вопрос - «Что делать? Как обезопасить систему ДО?»

Существует несколько способов защиты, которые формально можно разделить на два вида - технические и юридические. В данной статье мы остановимся на технических мерах защиты, юридическому аспекту будет посвящена другая статья. Заранее оговоримся, что лишь их совокупность даст большую вероятность безопасности и гарантированной защиты от плагиата, но не максимальную.

Итак, технические способы защиты очень разнообразны и зависят от состояния технического прогресса. Одним из древнейших способов такой защиты от незаконного копирования является уведомление общества о принадлежности авторских прав, заключающееся в нанесении на каждый экземпляр произведения информации об авторе и правообладателе. В соответствии со ст. 9 закона РФ «Об авторском праве и смежных правах» - для оповещения о своих правах автор вправе использовать [3]:

- знак охраны авторского права в виде латинской буквы «С» в окружности;
- имени (наименования) обладателя исключительных авторских прав;
- года первого опубликования произведения.

В некоторых случаях оправдано нанесение на экземпляры произведений дополнительной информации этического и воспитательного характера.

Другими словами, размещая учебные материалы на сайте, вы должны заранее побеспокоиться о наличии знака копирайта на предлагаемых учебных файлах, будь то Word - документы, HTML- страницы или иные формы представления информации. Это поможет вам не только защитить предлагаемые материалы, но и в случае прецедентов плагиата, доказать авторство в суде.

Хотя не гарантирует частичного копирования или замены (удаления) знака охраны, поэтому дополнительно следует обезопасить себя специальным паролем на редактирование.

Представление теоретической информации в наиболее безопасном формате, например, pdf - файлами программы Acrobat Reader или в графическом виде, т.е. в форматах jpg, gif и др. В этом случае делается снимок материала с указанием авторства, удалить которое будет более проблематично. Часто применяется кодирование и декодирование информации. Максимально защитить лекционный материал вы сможете, представив его в виде видео- или аудиоролика, это может быть лекция, наговоренный теоретический материал, визуальные лабораторные работы и т.д.

На бумажном носителе могут применяться технологии печати, которые исключают сканирование либо ксерокопирование произведения. Это может также достигаться путем применения специальной бумаги или особой люминесцирующей краски. От копирования страниц вы можете защититься, проставив копирайта на каждой странице. Различного рода пособия рекомендуется снабжать примерами с диска, который предоставлять отдельно или в

комплекте с пособием. Тут следует упомянуть об использовании кода ISBN – международный стандартный книжный номер. Это официальная, международно-признанная форма регистрации, которую используют издатели, книготорговцы и библиотеки для заказа, составления списков и складского учета.

Особое место занимают программные продукты: компьютерные программы, скомпилированные приложения, скрипты, мультимедийные энциклопедии, системы управления базами данных (СУБД), тестовые системы и т.д. Здесь методы защиты зависят от вида представления.

1. Сетевые системы (клиент-серверные технологии: СУБД, сетевые тесты, серверные скрипты и др.) являются наиболее защищенными со стороны авторского права (пользователь вынужден постоянно обращаться к автору), но больше подвержены хакерским атакам. Методы: программная блокировка копирования охраняемого материала на компьютер пользователя, использование программ клиентского места в совокупности с современными способами сетевой аутентификации и хранением пароля в базе данных на сервере, а не прописываемый в коде.

2. Конечные электронные продукты (приложения, локальные скрипты, электронные произведения и др.). Методы: прописывание копирайта в коде, блокировка или удаление программы после истечения срока пользования, закрытие доступа просмотра кода программы (php, html, Java, Perl...).

Также рекомендуется использовать, особенно в случае работы с электронными произведениями, технологию передачи прав [4]: предоставление доступа на определенное время нескольким пользователям обращаться к одному и тому же экземпляру электронного произведения, притом, что лишь один человек имеет доступ к нему в тот или иной момент. Например, пользователь загрузил на свой компьютер электронную книгу, после чего захотел дать её кому-нибудь почитать. Программное обеспечение, регулирующее цифровые права в экземпляре пользователя может позволить передать это произведение кому-либо на время или навсегда. В этом случае передается не только экземпляр электронной книги, но и право на ее просмотр. Несмотря на то, что физически копия книги остается в компьютере пользователя, он не сможет ее прочитать в течение того времени, на которое он её передал. По окончании периода проката, пользователь вновь получает это право. А копия книги деинсталлируется, т.е. файл физически исчезнет из памяти компьютера.

3. Лазерные компакт-диски, DVD, видео- и аудиокассеты. Методы: конечно, лицензирование, устанавливается в виде голографических наклеек высокого качества, принятия пользователем соглашения при установке программного обеспечения, программные способы блокировки перезаписи и копирования, подтверждение регистрации по Internet, постоянное обновление.

Для этих целей существуют компании, предлагающие регистрацию авторских прав. В большинстве стран не существует государственных и или полугосударственных органов, регистрирующих авторские права. Исключением являются Соединенные Штаты Америки. У них есть сайт www.copyright.gov. В Великобритании есть ведомство интеллектуальной собственности — www.ipo.gov.uk — это невероятно полезный сайт, но он не выполняет функции регистратора.

Есть много независимых коммерческих организаций, которые вы можете найти в интернете, которые предлагают выступить в качестве регистратора ваших авторских прав за

небольшую плату. И появился целый ряд компаний, предлагающий услуги по удалению пиратского контента. Они стали настолько популярными и успешными, что даже книгоиздатели активно пользуются их услугами.

В отличие от компаний, о которых мы говорили раньше, предлагающих регистрацию авторских прав, они предлагают более активные действия по защите ваших материалов. Вместо того чтобы просто регистрировать ваши авторские права, они активно ведут борьбу по недопущению распространения вашего материала в сети. Некоторые пошли еще дальше. Без вашего непосредственного участия и принятия вами решений, они круглосуточно следят за возможным явлением нарушения ваших прав. Поиск в интернете предоставит вам огромный выбор подобного рода компаний.

В заключении оговоримся, что, как показывает опыт, каждое усовершенствование технологий защиты приводит к усовершенствованиям хакерских методов, и что ни одна технология не застрахована от взлома. И поскольку не приходится ожидать появления абсолютно надежных технологий, то, по крайней мере, можно объявить действия хакеров и обход средств защиты нарушением закона. И в случае возникновения прецедентов плагиата должно быть представлено юридическое подтверждение ваших прав.

Список литературы

1. *Орехов, В.* Через тернии к знаниям [Электронный ресурс] / В. Орехов, А. Семенов. – Режим доступа: <http://www.i2r.ru/>.
2. *Кликунов, Н.Д.* Системные риски, порождаемые развитием дистанционного высшего образования в России [Текст] / Н.Д. Кликунов // Университетское управление: практика и анализ. – 2003. – № 5/6 (28). – С. 78.
3. Закон Российской Федерации «Об авторском праве и смежных правах» [Электронный ресурс]. – Режим доступа: <http://www.i2r.ru/>.
4. *Секор, Г.* Авторское право в цифровой среде и в Интернет: Точка зрения американских юристов [Электронный ресурс] – Режим доступа: http://active.wplus.net/copyright-monitoring/e-publish_sec03.html.

УДК 37:372.016:004

М.О. Чусавитин, Г.Н. Чусавитина МОДЕЛЬ МЕТОДИКИ ФОРМИРОВАНИЯ У БУДУЩЕГО УЧИТЕЛЯ ИНФОРМАТИКИ КОМПЕТЕНЦИИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Чусавитин Михаил Олегович

inform@masu-inform.ru

Чусавитина Галина Николаевна

gala_m27@mail.ru

ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», Россия, г. Магнитогорск

MODEL METHOD OF FORMING THE COMPETENCE OF INFORMATION SECURITY AT FUTURE DATE SCIENCE TEACHERS

Chusavitin M.O.

Chusavitina G.N.