базирующейся на понятии общего (коллективного) открытого ключа. Они обладают тем качеством, что размер подписи не увеличивается пропорционально числу подписавших участников. В дальнейшем необходимо рассмотреть вопросы стойкости предложенных схем к различным типам атак.

ПЕРЕЧЕНЬ ССЫЛОК

1. *Min-Shiang Hawng, Cheng-Chi Le.* Research issues and challenges for multiple digital signature // Int. J. of Network Security. – 2005. – Vol. 1, No 1. – P. 1–7.
2. *Молдовян Н. А., Молдовян П. А.* Новые протоколы слепой подписи // Безопасность информационных технологий. – М.:МИФИ. –2007. – № 3. – С. 17–21.
3. *Артамонов А. В., Маховенко Е. Б.* Применение алгоритма Шнорра в протоколе коллективной подписи // Материалы XIV Всероссийской научной конференции «Проблемы информационной безопасности в системе высшей школы». – 2007. – С. 17–18.
4. *Гортинская Л. В., Молдовян Н. А., Козина Г. Л.* Реализация протоколов коллективной подписи на основе стандартов ГОСТ 34.310–95 и ДСТУ 4145-2002 // Правове, нормативне та метрологичне забезпечення системи захисту інформації в Україні. – Киев: НТУУ «КПІ». – 2008. – № 1. – С.21–25.
5. *Карякин Ю. Д.* Технология «AXIS-2000» защиты материальных объектов от подделки // Управление защитой информации. – Минск: Институт технической кибернетики АН Белоруссии. – 1997. – Т. 1, № 2. – С. 90–97.
6. *Anna Nelasa, Victor Dolgov, Anatolij Pogorily.* Digital Signature Protocol for corporate network // Proceedings of International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2008). – Lviv-Slavsko (Ukraine). – 2008. – Pp. 396–397.
7. *A. Menezes, Y. Wu, R. Zuccherato.* An Elementary Introduction to Hyperelliptic Curves – Springer-Verlag, Berlin (Germany), 1998. – 31 p.
8. *D. G. Cantor.* Computing in Jacobian of a Hyperelliptic Curve // In Mathematics of Computation, volume 48 (177). – January 1987. – P. 95–101.
9. *Неласая А. В.* Протокол цифровой подписи на гиперэллиптических кривых // Радіоелектроніка. Інформатика. Управління. – Запорожье: ЗНТУ. – 2006. – № 1. – С. 113–118.

Після доробки 17.03.2008

В статті пропонуються нові протоколи колективного цифрового підпису на еліптичних та гіпереліптичних кривих. Обчислювальні схеми проілюстровані на прикладах.

New collective digital signature protocols on elliptic and hyperelliptic curves are proposed. Computational algorithms are illustrated with numerical examples.

УДК 65.012.8(043)

В. И. Слепцов, Л. М. Карпуков

ПРАВОВАЯ ПОДГОТОВКА КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются некоторые вопросы правовой подготовки специалистов по направлениям, входящим в отрасль знаний «Информационная безопасность», с учетом специфики их будущей профессиональной деятельности, учебных задач, законодательства Украины и опыта работы кафедры защиты информации Запорожского национального технического университета.

ВВЕДЕНИЕ

Уровень информационной безопасности, как в государственных структурах, так и в сфере хозяйственной деятельности, во многом определяется качеством подготовки работающих там специалистов, получивших образование по различным направлениям, объединяемым областью знаний «Информационная безопасность». Эффективность их усилий, направленных на защиту интересов субъектов информационных отношений зависит, прежде всего, от умения выявлять и оценивать угрозы, определять состояние защищенности информации, обоснованно выбирать способы ее защиты от совокупности реальных угроз, разрабатывать и внедрять системы защиты на основе требований законодательства Украины.

Базовые теоретические знания с получением необходимых практических навыков студенты, обучающиеся в ЗНТУ по специальностям «Защита информации в компьютерных системах и сетях» и «Системы защиты от несанкционированного доступа», приобретают при изучении дисциплин: «Основы информационной безопасности», «Физико-технические методы защиты информации», «Организационно-техническое обеспечение систем защиты информации», «Криптографические методы защиты информации» и др. Не возникает особых проблем при определении объема лекционного материала, методологии преподавания, если речь идет о традиционных вопросах, связанных с изучением технических каналов утечки информации и методов их закрытия, программно-аппаратных способов получения несанкционированного доступа к защищаемой информации, обрабатываемой в информационно-теле-

коммуникационных системах, и механизмах защиты от НСД, которые рассматриваются в этих курсах. В то же время, вследствие отсутствия принятой на государственном уровне программы подготовки по защитным специальностям до настоящего времени у специалистов и преподавателей вузов не сложилось единого представления, во-первых, о небходимости включения в рабочие программы обучения дисциплины, включающей в себя вопросы правового обеспечения деятельности в области защиты информации, и, во-вторых, о тематике курса. Содержание изданных учебных пособий [1,2] так же не дает возможность сформировать хотя бы концептуально общий подход к объему и характеру сведений в области правовой защиты информации, необходимых для качественной подготовки бакалавров, специалистов и магистров.

На кафедре защиты информации ЗНТУ с первого года подготовки специалистов в сфере защиты информации в рабочие программы включено изучение дисциплины «Правовые основы защиты информации». При этом авторы программы исходили из неоспоримости утверждения, что легитимность (а в некоторых случаях и действенность) использования любых организационных и технических средств защиты определяется их соответствием нормативно-правовой базе, сложившейся в государстве. Следовательно, без знания системы и основных норм информационного законодательства Украины любая деятельность в сфере защиты информации зачастую приобретает не правовой характер с вытекающими отсюда негативными последствиями. Ниже изложены те подходы к формированию содержания указанного курса и методологии преподавания, которые использованы в ЗНТУ и которые, как нам видится, могут быть предметом обсуждения в вузовской и инженерной среде.

ОБОСНОВАНИЕ ПОДХОДА К ФОРМИРОВАНИЮ ПРОГРАММЫ ДИСЦИПЛИНЫ

Исходя из достаточно универсального подхода к изучению любой отрасли знаний: идти от общего к частному, рабочая программа дисциплины «Правовые основы защиты информации» предполагает рассмотрение в порядке очередности следующих базовых тем:

1. Общая характеристика информации и принципов правового обеспечения информационной безопасности.

2. Информационное законодательство Украины.

3. Правовое регулирование информационных отношений между субъектами в информационных системах.

4. Законодательство Украины в сфере защиты государственной тайны.

5. Правовое регулирование электронного документооборота.

6. Лицензирование хозяйственной деятельности в сфере защиты информации.

7. Сертификация средств ТЗИ и КЗИ на соответствие требованиям обеспечения безопасности информации.

8. Правовое регулирование отношений, которые касаются творческой деятельности.

Какие же задачи ставились кафедрой при наполнении каждой из названных тем конкретным содержанием, и на какой методологической основе это осуществлялось?

Тема № 1. Поскольку дисциплина изучается в рамках первого года подготовки специалистов указанных выше специальностей, в этой части курса студентам, которые впервые сталкиваются с научным подходом к постановке проблем обеспечения информационной безопасности и возможностями их решения, даются не только сведения, характеризующие информацию, как объект правовой защиты, но и характеристику: существующих в информационном поле взаимодействия субъектов угроз; способов и методов их нейтрализации; понятия «информационная безопасность»; критериев и категорий защищенности информации. При этом упор делается на усвоении будущими специалистами базового подхода к обеспечению информационной безопасности, основывающегося на том, что защита информации не является самоцелью, а следствием осознания субъектами информационных отношений необходимости защиты своих прав от возможных посягательств на них в виде реализации угроз различного характера.

Вторым важным постулатом, которому, по нашему мнению, необходимо уделить особое внимание, – это признание главенствующей роли государства в защите прав всех участников информационного взаимодействия, не выходящего за пределы правового поля. Такая роль, как известно, основывается на разработанной государственной политике обеспечения информационной безопасности, основные положения которой рассматриваются в рамках курса. Отсюда вытекает необходимость характеристики организационной государственной структуры – системы ТЗИ в Украине, обеспечивающей реализацию этой политики. В результате рассмотрения указанной темы у студентов должно сложиться четкое представление о проблемах, существующих в сфере обеспечения информационной безопасности, путях их решения, роли государства в защите прав законных участников информационных процессов.

При изучении темы № 2 основное внимание, по нашему мнению, следует уделить обоснованию приоритетности решения задачи защиты интересов субъектов информационных отношений на основе нормативно-правового регулирования этой деятельности во всех ее аспектах с общей характеристикой той правовой базы,

которая сложилась на данный момент в Украине. В этом контексте рассматриваются избранный в нашем государстве способ классификации информационного законодательства, его преимущества и недостатки, а так же источники информационного права. При этом подчеркивается роль Основного закона Украины – Конституции, конкретные нормы которой прямо защищают основные права участников информационных процессов и определяют условия, при которых возможно ограничение этих прав. При рассмотрении этой темы внимание студентов также обращается на существующие пробелы в информационном законодательстве Украины, его противоречивость в отдельных аспектах, на существующие возможности его реформирования [1–3].

Отдельного рассмотрения требуют нормы закона Украины «Об информации», являющегося базовым в информационном праве, который заложил правовые основы защиты информации с ограниченным доступом. Здесь основное внимание уделяется таким вопросам как: характеристика структуры информационных отношений и принципы их правового регулирования; виды информационных ресурсов и право собственности на них; виды режима доступа к информации и ее классификация в соответствии с режимом доступа; основания возникновения ответственности за нарушения законодательства и виды такой ответственности. Поскольку наличие уголовной ответственности за отдельные нарушения является наиболее эффективной мерой защиты законных интересов владельцев и пользователей информационных ресурсов, в рамках курса рассматриваются те виды преступлений (предусмотренных криминальным кодексом Украины), предметом которых является информация или поддерживающая ее инфраструктура [2]. Это, в свою очередь, требует формирования у студентов некоторых представлений, связанных с уголовным правом, в частности, понятия преступления и субъекта преступления (с разделением субъектов на виды), состава преступления и виды составов, основания привлечения лица к уголовной ответственности и формы вины. Практика показала, что наиболее эффективной формой изучения конкретных составов преступлений, которые могут совершаться в информационной сфере, является разбор студентами этих составов на практических занятиях с использованием демонстрационных материалов в виде плакатов или слайдов, на которые выведены диспозиция и санкции конкретной статьи КК Украины.

Необходимое внимание уделяется получению студентами представлений о правах и обязанностях спецслужб при осуществлении скрытого доступа к интересующей их информации, принципах оперативно-розыскной деятельности (ОРД), гарантиях законности во время осуществления такой деятельности [4]. Акцент при изучении этих вопросов делается на недопустимости, с точки зрения требований законодательства Украины, использования специальных методов и средств ОРД не уполномоченными на то структурами или физическими лицами [5].

Давая в целом положительную оценку закону Украины «Об информации» и характеризуя его роль в вопросах правового регулирования информационных отношений, в лекционном курсе одновременно подчеркивается, что этот законодательный акт не в полной мере отвечает современному уровню развития отношений в сфере информационной деятельности. В частности, регулирование отношений в таких сферах, как информация о личности, информация для служебного пользования требует дальнейшего развития на основе разработки и принятия соответствующих законодательных актов [6]. Неопределенными до настоящего времени являются положения действующего законодательства в отношении секретной информации, не составляющей государственной тайны. Накопленный опыт свидетельствует, что если «не уходить» от подобных вопросов, а ставить их перед студентами в рамках изучаемого курса, это поднимает их интерес к правовой проблематике обеспечения информационной безопасности, способствует более глубокому усвоению материала.

Основным средством, обеспечивающим на современном этапе развития общества эффективное информационное взаимодействие между субъектами, являются информационно-телекоммуникационные технологии, обеспечивающие практически все процессы создания, распространения и использования информации. Это влечет за собой необходимость разработки правовых норм, определяющих правила работы с информационными ресурсами, ответственность за их создание и сохранность, за обеспечение их достоверности, а также механизмы пресечения общественно-опасного поведения в их использовании. Правовые нормы указанных типов относятся к проблематике информационного права, и их достаточно детальное рассмотрение является, по нашему мнению, насущной необходимостью. При этом важно указать, что главной особенностью правового регулирования в этой сфере является его опора на совершенно новые для теории права и государства понятиях («компьютер», «информационные ресурсы», «база данных», «вычислительная сеть», «электронная цифровая подпись» и т. д.) [7]. Рассмотрение вопросов правового регулирования отношений между субъектами, являющимися законными пользователями автоматизированных систем обработки информации (АС), осуществляется на основе Украины «О защите информации в АС». Основные положения этого закона, касающиеся характеристике угроз информационной безопасности АС, объему прав различных категорий пользователей АС, требований к обеспечению защиты информации, которая обрабатывается в АС, правовой основы создания службы защиты ин-

формации и определения ответственности за правонарушения в сфере использования компьютерных технологий излагаются в лекционном курсе, опираясь на тот объем сведений в сфере компьютерных технологий, которыми располагают студенты в соответствии с программой их обучения. Затем, привязываясь к названному закону, рассматривается порядок защиты государственных информационных ресурсов в информационно-телекоммуникационных системах, определенный соответствующим НД ТЗИ.

Перед изложением базовых положений закона Украины «О государственной тайне» обосновывается особая важность эффективной организации защиты такого вида информации ограниченного доступа, как государственная тайна, утечка которой предполагает нанесения вреда национальным интересам Украины. Неоднократно подчеркивается, что защитные мероприятия должны реализовываться в строгом соответствии с нормами этого закона, достаточно четко регламентирующими все процессы, происходящие в этой сфере, начиная от отнесения информации к категории государственная тайна и заканчивая контролем за соблюдением режима секретности. Этим обуславливается необходимость усвоения студентами таких вопросов как: порядок отнесения информации к государственной тайне; порядок засекречивания и рассекречивания материальных носителей секретной информации; получение прав допуска и доступа к секретной информацией или к работам, с ней связанным; понятие режима секретности и меры по его обеспечению.

Все более широкое использования абонентами компьютерных сетей технологии обмена документами в электронной форме требует знания от специалистов в области обеспечения информационной безопасности юридических аспектов электронного документооборота и возможности использования для подтверждения неизменности и аутентичности электронных документов электронной цифровой подписи (ЭЦП). По этой причине необходимое внимание уделяется изложению основных положений законов Украины «Об электронных документах и электронном документообороте», «Об электронной цифровой подписи». Раскрываются правовые понятия электронного документа и ЭЦП, их статус. Дается характеристика действующей в Украине системе сертификации открытых ключей, особенностей использования ЭЦП в зависимости от статуса сертификата открытого ключа. В то же время, на наш взгляд, нельзя не упомянуть о наличии существенных отклонений названных законов в части определения базовых терминов от законодательства и Директивы ЕС, что может привести к недоразумениям и к неопределенности при использовании этих законодательных актов и к возможным правовым коллизиям на межгосударственном уровне.

Поскольку практически вся хозяйственная деятельность в области технической и криптографической защиты информации подлежит согласно действующему законодательству государственному регулированию, не вызывает сомнений необходимость изложения некоторых норм Закона Украины «О лицензировании определенных видов хозяйственной деятельности», выделяя такие вопросы как: характеристика государственной системы лицензирования; порядок лицензирования; контроль в сфере лицензирования. Отталкиваясь от этих базовых вопросов, далее дается достаточно подробная характеристика системы государственного лицензирования деятельности в области защиты информации, являющейся необходимым элементом национальной системы ТЗИ. Излагаются требования нормативных документов, определяющих перечень видов деятельности в сфере защиты информации, подлежащих лицензированию, особенности лицензирования, характеристика лицензионных условий и порядок контроля за их соблюдением.

Освоение студентами темы, связанной с правовыми основами проведения сертификации технических и криптографических средств защиты информации, предполагает так же ознакомление их с общими правилами подтверждения соответствия, сформулированными в Законе Украины «О подтверждении соответствия» и в декрете КМ Украины «О стандартизации и сертификации». На этой базе далее рассматриваются требования действующих нормативных документов в отношении сертификации средств ТЗИ и КЗИ, а именно: распределение ответственности в системе УкрСЕПРО; организационная структура этой системы; порядок подготовки и проведения сертификации средств КЗИ и ТЗИ; права и обязанности органов сертификации и заявителей; перечень средств ТЗИ и КЗИ, которые подлежат обязательной сертификации; виды документов, подтверждающих соответствие; правовые последствия использования не сертифицированных или не прошедших государственную экспертизу средств обработки и защиты информации.

Важнейшим видом информации на современном уровне развития общества является информация, полученная в результате творческой деятельности, поскольку результаты, например, научно-технической деятельности во многом определяют темпы развития цивилизации, обеспечивают при наличии соответствующих условий достижение высокого уровня экономического развития страны и благосостояния ее граждан. Отсюда вытекает необходимость четкого правового регулирования отношений, возникающих в сфере научно-технического творчества и использования его результатов. Так как эти результаты всегда представляют собой конкретные документированные сведения (описание изобретений или полезных моделей) или формализованное изложение выводов, полученных в ходе мысли-

тельной деятельности, патентное и авторское право в определенной части можно считать частью информационного права, по крайней мере, если мы говорим о защите неимущественных прав авторов. На основе таких соображений в рамках дисциплины рассматриваются сновные положения Законов Украины «Об авторских и смежных правах» и «Об охране прав на изобретения и полезные модели». При этом акцентируется внимание студентов на принципиальном различии объектов правового регулирования в авторском и патентном праве при схожести подходов к защите прав авторов как произведений, так и результатов изобретательской деятельности.

Проведение практических занятий, с целью надежного закрепления знаний, полученных студентами в ходе слушания лекций по данной дисциплине и в процессе самостоятельной подготовки, осуществляется в форме заслушивания рефератов, подготовленных студентами по темам, требующим более обстоятельного рассмотрения, чем это сделано (ввиду недостатка времени) при чтении лекций, и путем решения студентами практических задач, вытекающих из рассмотренных вопросов.

ВЫВОДЫ

Востребованность специалистов в области защиты информации определяется уровнем их подготовки, позволяющей решать (в числе прочих) практические задачи по предупреждению или нейтрализации существующих угроз информационной безопасности. Достаточный уровень подготовки таких специалистов может быть достигнут только с учетом необходимости усвоения ими базовых знаний в области правового регулирования многообразной деятельности, конечной целью которой является защита интересов законных участников информационных процессов. Это является гарантией не только законности такой деятельности, но, что не менее важно, и ее эффективности.

Предлагаемый подход к формированию программы и методики обучения, разумеется, не является единственно возможным. Авторы предполагают возможность существования других концепций, на основе которых возможно построения курса, посвященного правовым основам защиты информации. Прежде всего, речь, по-видимому, может идти о другом видении программы дисциплины, ее структуры, акцентах. Возможно, большее внимание следует уделить таким вопросам, как: формирование информационной культуры, как объекта информационного права; международным аспектам информационного права; роли информации в общественных отношениях на разных исторических этапах развития общества и т. д. [1], оставляя некоторые из названных выше тем для самостоятельного изучения студентами. Цель, которая преследовалась авторами при написании этой работы, будет достигнута, если данная статья послужит одним из поводов для активизации дискуссии по данной проблематике.

ПЕРЕЧЕНЬ ССЫЛОК

1. *Цимбалюк В. С., Гавловський В. Д., Гриценко В. В. та ін.* Основи інформаційного права України.: Навч. посіб. / О-72. – К.: Знання, 2004. – 274 с.
2. *Голубев В. І., Гавловський В. Д., Цимбалюк В. С.* Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій.: монографія. – Запоріжжя: Просвіта, 2001. – 252 с.
3. *Гавловський В. Д., Гуцалюк М. В., Цимбалюк В. С.* Електроний бізнес та концепція реформування системи інформаційного законодавства України // Бизнес и безопасность. – 2001. – № 4. – С. 2–4.
4. Планов С. А. Негласное получение информации (нормативно-правовое эссе) // Бизнес и безопасность. – 2003. – № 4 – С. 9–12.
5. *Пиза Д. М., Слепцов В. И.* Информационная безопасность. Вопросы подготовки кадров // Радіоелектроніка, інформатика, управління. – 2005. – № 2.
6. *Ботвінкін О. В., Ворожко В. П.* Інформація з обмеженим доступом, що не є державною таємницею, в законодавстві України. Аналітичний огляд. – Київ.: НА СБ України, 2006. – 96 с.
7. *Загородников С. Н., Шмелев А. А.* Организационное и правовое обеспечение информационной безопасности. Часть 1 // Приложение к журналу «Информационные технологии». – 2005. – № 12. – С. 5–7.

Надійшла 5.06.2008
Після доробки 9.06.2008

Розглядаються деякі питання правової підготовки фахівців з напрямків, що входять в галузь знань «Інформаційна безпека», з урахуванням специфіки їх майбутньої професійної діяльності, учбових завдань, законодавства України і досвіду роботи кафедри захисту інформації Запорізького національного технічного університету.

Some questions of legal preparation of specialists are examined on directions, to included in the field of knowledges «Informative safety», taking into account the specific of their future professional activity, educational tasks, legislation of Ukraine and experience department of priv the Zaporozhia national technical university.