V. S. Bedrin

К ВОПРОСУ ФОРМИРОВАНИЯ ИНФОРМАЦИОННО-ПРАВОВОЙ КУЛЬТУРЫ ВЫПУСКНИКА ВОЛГОГРАДСКОЙ АКАДЕМИИ МВД РОССИИ

В статье рассматриваются вопросы формирования информационно-правовой культуры выпускника Волгоградской академии МВД России, его подготовки к реализации правовых норм в области информационных отношений.

Ключевые слова: информационная безопасность, защита информации, системы шифрования, информационные ресурсы, ситуации практической направленности.

V. S. Bedrin

ABOUT SHAPING OF THE INFORMATION LEGAL CULTURE OF A GRADUATE OF THE VOLGOGRAD ACADEMY OF THE MINISTRY OF INTERIOR OF RUSSIA

In the article the author focuses on the issues of shaping the information legal culture of a graduate of the Volgograd Academy of the Ministry of Interior of Russia, in particular his preparation for implementing legal norms in the sphere of information relations.

Keywords: information security, information protection, enciphering system, information resources, practice-related situations.

При современных темпах развития информационных технологий, систем связи и коммуникаций проблема формирования научно обоснованной системы обеспечения информационной безопасности становится все более актуальной.

В условиях нарастающей глобализации информационная сфера во все возрастающей степени становится не только ареной международного сотрудничества, но и полем противоборства. Всестороннее вовлечение России в процесс формирования глобального информационного пространства превращает обеспечение информационной безопасности страны в одну из важнейших стратегических задач государства.

Одной из крупных государственных проблем является недостаточная защищенность информационных ресурсов от

несанкционированного доступа, которая крайне негативно влияет на обеспечение безопасности информационных и телекоммуникационных систем, используемых в различных сферах общественной жизни и государственной деятельности.

Одним из важнейших направлений обеспечения информационной безопасности является дальнейшее развитие сбалансированной системы организационно-технических и программных методов защиты информации, направленных на противодействие и нейтрализацию угроз интересам личности, общества и государства в целом.

В этой связи особенно остро стоит вопрос о необходимости подготовки кадров, не только обладающих компьютерной грамотностью, но и проявляющих профессиональную компетентность в квалифицированной и надежной защите

информационных ресурсов Российской Федерации. Немалый вклад в это общегосударственное дело должны будут внести и будущие сотрудники органов внутренних дел.

Общеобразовательная подготовка сотрудников правоохранительной сферы в области информационных технологий, проводимая в рамках дисциплины «Математика и информатика», должна быть дополнена их обучением по более профильной и профессионально ориентированной дисциплине «Основы информационной безопасности в органах внутренних дел».

В этой связи на кафедре информатики и математики Волгоградской академии МВД России уже не первый год курсантам и слушателям преподается данная дисциплина, которая относится к специальным курсам по выбору обучаемого вузовского компонента государственного образовательного стандарта по специальностям 030501.65 — «Юриспруденция», 030505.65 — «Правоохранительная деятельность». Преподавание дисциплины предполагает, что к началу ее изучения обучаемые уже имеют представления об основных возможностях компьютерной техники и современных телекоммуникаций, овладели умениями управлять работой компьютера на основе операционной системы Microsoft Windows и обрабатывать служебную информацию с помощью приложений пакета Microsoft Office.

Тематическим планом предусмотрено изучение трех тем, а именно «Организационно-правовые основы защиты информации в ОВД», «Организационно-технические и программные методы защиты информации в компьютерных системах» и «Защита информации от утечки на объектах информатизации российских и зарубежных правоохранительных органов». Весь лекционный материал сопровождается мультимедийной поддержкой (презентациями), где рассматриваются практически все базовые

понятия и принципы информационной безопасности, приведены необходимые классификации методов защиты информации, дается представление о правовых основах создания и использования систем физической защиты объектов информатизации.

На практических занятиях обучаемые, помимо выполнения заданий для самостоятельной работы, анализируют ситуации практической направленности, что позволяет актуализировать их проблемно-творческое мышление. Данные ситуации требуют не односложных ответов, а логических рассуждений, обращения к законам и подзаконным нормативно-правовым актам в справочно-правовых системах «Консультант-Плюс» и «Гарант», принятия грамотных решений в условиях профессиональных коллизий. Для углубленного понимания подходов и методов по обеспечению информационной безопасности на занятиях используется метод обучения, названный Security Roadmap, когда обучаемым в наглядном виде на примере объекта информатизации (компьютерный класс) демонстрируются место и роль средств безопасности.

В структуру курса «Основы информационной безопасности в ОВД» входит рассмотрение следующих базовых вопросов:

- организация систем защиты информации; управление безопасностью, в том числе нормативно-правовое обеспечение; безопасность на физическом и логическом уровнях; методология и документирование;
- основные цели и направления, методы и средства защиты информации; виды угроз безопасности и их характер;
- криптографические средства, их место в системе обеспечения информационной безопасности компьютерных систем;
- программные средства обеспечения безопасности операционных систем, банков данных, сервисов сети Интернет; средств анализа безопасности при обнаружении атак, а также проблемы применения цифровой подписи;

— виды информационных ресурсов, а также основные компоненты автоматизированных информационных систем, используемые в органах внутренних дел.

В качестве программных средств защиты информации обучаемые изучают четыре группы систем:

— системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей (применяются для ограничения доступа случайных и незаконных пользователей к ресурсам компьютерной системы);

— системы шифрования дисковых данных (осуществляют криптографические преобразования данных на уровне файлов или на уровне дисков. В качестве программ первого типа изучаются функциональные возможности архиватора WINRAR, который позволяет использовать криптографические методы для защиты архивных файлов, а второго типа — возможности программы Diskreet, входящей в состав популярного программного пакета Norton Utilities, Best Crypt);

— системы шифрования данных, передаваемых по сетям (рассматриваются два основных способа шифрования: канальное шифрование (защита полного объема информации, передаваемой по каналам связи, включая служебную) и оконечное (абонентское) шифрование (обеспечивает конфиденциальность содержания сообщений, передаваемых между двумя абонентами, вся служебная информация остается открытой);

— системы аутентификации электронных данных (установление подлинности автора и проверка отсутствия изменений в полученном по сети документе).

Функциональные возможности автоматизированных информационных систем (АИС), используемых в органах внутренних дел, на занятиях рассматриваются на базе АИС «Марафон». На основе материала учебной фабулы уголовного дела обучаемые, используя интегрированные информационные ресурсы данной системы для установления

личности всех участников совершенного преступления, работают с картотекой, делают запросы по лицам, документам, транспортным средствам, оружию и т. д.

Любая педагогическая технология — это информационная технология. Информационные технологии в образовании использовались всегда. С появлением компьютеров они начали широко использоваться и в учебном процессе вузов, что дало толчок для появления технологии «информационные технологии обучения», а немного позже и термин «новые информационные технологии» (НИТ).

Известно, что НИТ включают в себя: интеллектуальное обучение; программное обучение; экспертные системы; имитационное и дис-танционное обучение; мультимедиа и гипертекст; обучающие и тестирующие системы; справочно-правовые системы и т. д. Для повышения качества образования на основе НИТ в процессе преподавания дисциплины «Основы информационной безопасности в ОВД» на кафедре используется ряд методик НИТ (о некоторых шла речь выше). Немалое внимание на практических и консультационных занятиях уделяется работе обучаемых с электронными учебно-методическими материалами (фондовые лекции, планы семинарских и практических занятий, учебные пособия и т. д.). Эффективно применяются такие виды текущего и итогового контроля знаний, как экспресс-опрос (в форме письменной контрольной работы («летучка») в течение 3—5 минут) и тестовые компьютерные программы, что позволяет экономить учебное время и увеличивать число опрашиваемых, а также улучшать качество обучения и глубину остаточных знаний.

Формирование информационно-правовой культуры выпускников вузов МВД России является крайне актуальным для деятельности министерства в современных условиях: с одной стороны, выполняющего практически весь комплекс мероприятий по обеспечению информационной безопасности государства,

связанных с борьбой с преступлениями в области высоких технологий, а с другой — способного эффективно решать свои задачи в условиях обеспечения собственной информационной безопасности.

© В. С. Бедрин, 2010