Поскольку работа системы требует наличие базы данных (БД), для начала необходимо создать и настроить БД. Данные в базе находятся под управлением СУБД MySQL 5. В БД имеется несколько таблиц. Отдельно создается таблица пользователей (тестируемых), непосредственно таблица с вопросами, а также таблица для редактора формул, в которой будут храниться определенные материалы предметной области (формулы).

Весь комплекс имеет так называемую панель управления (с привилегиями преподавателя или администратора), с помощью которой можно управлять всем комплексом в целом. После создания БД необходимо ее заполнить соответствующей информацией. Таблица пользователей заполняется непосредственно самими тестируемыми через web-форму, которая запрашивает определенную информацию. Заполнение таблицы вопросов и таблицы с формулами, созданными непосредственно редактором, курируется администратором.

Пройдя регистрацию, пользователь переходит к тестированию. При прохождении вопросов (примерное количество 50) система фиксирует время, которое потребовалось на прохождение каждого вопроса. С каждым последующим шагом суммируется время пройденных ранее вопросов и вычитается от общего времени, которое выделяется на прохождение всех тестов. Возможен выбор второго варианта временного учета (назначается преподавателем), при котором на каждый вопрос отводится примерно по одной минуте для ответа.

За выдачу и сортировку вопросов в базе отвечает специальный класс GenQuest, который имеет определенный набор интерфейсов для работы с БД (таблицей вопросов Question).

После прохождения тестов студенту выдается результат, который содержит оценку, перечень тем, на которые были даны правильные ответы (сильные фрагменты), и тем с неправильными ответами (слабые фрагменты). Результат прохождения отправляется преподавателю с указанием данных тестируемого (ФИО и т. д.) и его оценкой.

Один из режимов создания вопросов является создание вопроса с помощью редактора формул. Преимущество такого подхода в том, что созданная редактором формула фиксируется в базе, при ответе на такой вопрос студенту также предоставляется возможность ответить на формулу формулой с помощью редактора. Каждый элемент, созданный редактором, приобретает вид определенного объекта. При ответе на вопрос эти объекты анализируются на схожесть, и таким образом формируется ответ на вопрос.

Выполнив анализ и частичную реализацию системы дистанционного тестирования с подключаемым редактором формул, можно сделать выводы, что актуальность такой системы очень велика. Данная система ориентирована на конкретную предметную область и имеет ряд отличительных особенностей от других систем online-тестирования, к примеру по английскому языку. Одним из отличий является встроенный редактор формул, который раскрывает и доказывает эффективность дистанционного тестирования, расширяя возможности тестирования в целом.

Данную программную систему предлагается использовать в Харьковском национальном университете внутренних дел при проведении экзаменов и зачетов у курсантов и студентов, обучающихся по специальности 6.170102 «Системы технической защиты информации».

А.Н. Лепехин

О ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Парадигмальные изменения в процессах современной общественной жизни и связанные с ними преобразования в системе образования обусловливают определенные трансформации в технологиях обучения и содержании такой деятельности. Качественные изменения в структуре социальных интересов и возрастание роли виртуальной среды общения как средства коммуникации предопределяют широкое внедрение информационных технологий в жизнь членов общества. Наряду с положительными моментами информатизации возникают и негативные, связанные с противоправными посягательствами на информационные процессы. Указанные обстоятельства обусловливают необходимость подготовки специалистов, способных надлежащим образом реагировать на вызовы современности.

Вместе с тем в настоящее время в системе подготовки сотрудников правоохранительных органов не уделяется должного внимания изучению вопросов информационной безопасности. Отдельные вопросы криминалистического и оперативно-розыскного обеспечения раскрытия и расследования компьютерных преступлений рассматриваются в соответствующих дисциплинах. В то же время современные информационные технологии используются не только при совершении так называемых «компьютерных преступлений», но и при реализации преступного замысла по ряду других, где применение компьютерных технологий позволяет достичь криминальных целей. Данные факторы обусловливают необходимость проработки вопроса о преподавании основ информационной безопасности как на первой ступени получения высшего образования, так и в рамках системы повышения квалификации и переподготовки сотрудников правоохранительных органов.

Как предполагается, изучение вопросов информационной безопасности и их преломление на конкретную правоприменительную деятельность позволят более систематизировано использовать знания и умения, полученные по профильным дисциплинам (уголовное право, криминалистика и оперативно-розыскная деятельность) для их акцентуации на определенной сфере противоправной деятельности – преступлениях в сфере информационной безопасности. Полагаем, что преподавание основ информационной безопасности должно иметь отраслевой характер, т. е. вопросы уголовно-правового, криминалистического и оперативно-розыскного характера в сфере информационных технологий следует изучать в комплексе и в рамках одной (максимум двух) дисциплины. Тем самым будет достигнута специализация обучения, его практическая направленность и решение задач, стоящих перед правоохранительными органами в деле противодействия криминальным проявлениям в информационной сфере.

Полагаем, что целью изучения основ информационной безопасности будет являться формирование основ знаний и умений, необходимых будущим специалистам-практикам в области информационной безопасности. Для достижения указанной цели необходимо использовать комплексный подход, в рамках которого при изучении курса подлежат рассмотрению вопросы понятия и содержания информационной безопасности; системы защиты информации; правового и организационно-технического обеспечения информационной безопасности; угроз, методов и средств обеспечения информационной безопасности, а также оперативно-розыскного и криминалистического обеспечения информационной безопасности.

Следует отметить, что как самостоятельная категория общественных отношений информационная безопасность является сравнительно молодой, быстро развивающейся областью информационных технологий, для успешного освоения которой важно с самого начала усвоить современный, согласованный с другими отраслями научного знания информационный базис, включающий в себя основы информационных технологий, сетевое взаимодействие, программно-аппаратное обеспечение информационной безопасности и ряд других направлений информационного обеспечения функционирования компьютерных сетей и систем.

В результате изучения курса предполагается, что обучаемые должны знать понятие информационной безопасности и механизмы защиты информации; правовые основы обеспечения информационной безопасности; организационно-техническое обеспечение информационной безопасности; понятие, виды и каналы утечки информации; методы и средства обеспечения безопасности информации; краткую характеристику

противоправных деяний как основного фактора угрозы информационной безопасности; криминалистическую и оперативно-розыскную характеристику преступлений против информационной безопасности; силы и средства оперативно-розыскной деятельности, используемые при предупреждении и раскрытии преступлений в сфере информационной безопасности; основания и условия проведения оперативно-розыскных мероприятий при предупреждении и раскрытии преступлений в информационной сфере; способы обнаружения, фиксации и изъятия следов информационных преступлений; тактические особенности производства отдельных следственных действий по делам в сфере информационной безопасности; порядок назначения и производства судебных компьютерно-технических экспертиз по делам данной категории.

В итоге обучаемые должны уметь: проводить отдельные оперативно-розыскные мероприятия при предупреждении и раскрытии преступлений в информационной сфере; обнаруживать, фиксировать и изымать следы информационных преступлений; проводить отдельные следственные действия по делам в сфере информационной безопасности; назначать судебные компьютерно-технические экспертизы по делам данной категории, что обусловливает практическую направленность курса.

По нашему мнению, на изучение курса необходимо 80 аудиторных часов, из них: 22 часа – лекционные занятия, 18 – семинарские, 40 – практические. Форма контроля знаний – экзамен.

ТЕМАТИЧЕСКИЙ ПЛАН
учебного курса «Основы информационной безопасности»
для дневной формы обучения

№ п/п	Наименование разделов и тем дисциплины	Общее количество часов	Количество аудиторных часов					самостоятельная работа
			всего	лекции	семинары	практические	групповые упражнения	
Раздел 1 Государственная система защиты информации в Республике Беларусь								
1.	Защита информации в системе национальной безопасности Республики Беларусь	6	4	2	2			2
2.	Правовые основы обеспечения информационной безопасности	6	4	2	2			2
3.	Организационно-техническое обеспечение информационной безопасности	6	4	2	2			2