ПРОГРАММНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ТЕСТИРОВАНИЯ ПО ВОПРОСАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю.А. Гатчин, Б.А. Крылов

В статье изложены результаты работ, проводимых на кафедре проектирования компьютерных систем, по созданию комплекса дистанционного обучения по вопросам информационной безопасности, осуществляемых в рамках Федеральной целевой программы**:** "Развитие единой образовательной информационной среды", раздел: "Развитие информационных технологий сферы образования, научно-исследовательские и опытно-конструкторские работы" [1].

Введение

Интенсивное развитие средств информатизации, программного обеспечения в сочетании с аппаратными комплексами телекоммуникационных систем приблизило общество к качественно новому рубежу, когда информационные технологии будут определять и обеспечивать развитие общества. Сейчас уже невозможно представить работу учебных заведений, объединенных в единую образовательную среду, без внутренней инфраструктуры на базе компьютерных технологий и без выхода в глобальные информационные сети.

В этих условиях информационные ресурсы единой образовательной среды и каждой ее составляющей представляют собой огромную материальную и интеллектуальную ценность, несанкционированный доступ к которым может нанести существенный ущерб.

Возрастание количества видов и способов осуществления нарушения безопасности информации создает предпосылки для изменения требований к средствам защиты и специалистам по защите информации.

На основе проведенного анализа сформированы четыре категории специалистов по их отношению к информационной безопасности и уровню обеспечения информационной безопасности: Для каждой категории специалистов определены конкретные требования к уровню знаний специалистов по проблемам информационной безопасности.

Для интенсификации учебного процесса разработана и доведена до практического использования система дистанционного тестирования. В состав системы дистанционного обучения включено 13 тестовых заданий.

Требования к уровню необходимых знаний, вопросов, связанных с информационной безопасностью для категорий специалистов

I категория - специалисты, эпизодически сталкивающиеся с проблемами защиты информации – должны отвечать следующим квалификационным требованиям:

иметь представление

- о системе подхода к понятиям "защита информации", "информационная безопасность", "информационная война";
- об источниках и способах воздействия угроз на объекты информационной безопасности и ее субъектов хозяйствования;
- о правовом регулировании в области информационной безопасности;
- о перспективных направлениях развития теоретических основ информационной безопасности;

знать

- методологическое и технологическое обеспечение информационной безопасности;
- базовый понятийный аппарат в области защиты информации;
- принципы, методы и средства обеспечения информационной безопасности;
- особенности организационно-правового обеспечения информационной безопасности;
- систему сохранения государственной тайны;
- методы организации деятельности подразделений обеспечения информационной безопасности на предприятии;
- систему сертификации средств защиты и лицензирования деятельности в области информационной безопасности.

II категория – специалисты, постоянно занятые деятельностью, связанной с защитой информации, но не занимающиеся профессионально защитой информации – должны отвечать следующим квалификационным требованиям:

иметь представление

- об основах государственной политики и основных нормативных документах в области информационной безопасности;
- об источниках и способах воздействия угроз на объекты информатизации;
- о правовом регулировании в области информационной безопасности;
- о системе защищенного документооборота;

знать

- цели и значение защиты информации;
- виды уязвимости защищаемой информации и формы ее проявления;
- существующие угрозы безопасности информации;
- организационные методы защиты информации;
- правовые аспекты защиты информации;
- систему сохранения государственной и других видов тайн;
- делопроизводство и защищенный документооборот;
- носители защищаемой информации;
- кадровое обеспечение информационной безопасности.

III категория – специалисты, профессионально занимающиеся защитой информации – должны отвечать следующим квалификационным требованиям:

иметь представление

- о системе национальной безопасности РФ и, в частности, информационной безопасности;
- о законодательстве и нормативных актах в области информационной безопасности;
- о концептуальных моделях составления, распределения, обработки, исполнения, использования и хранения конфиденциальных документов в различных организационных структурах и с использованием различных технологических схем;
- о правовом регулировании в области информационной безопасности;

знать

- принципы, методы, системы и средства обеспечения информационной безопасности;
- формальные модели, лежащие в основе систем обеспечения информационной безопасности и их теоретические основы;
- стандарты и нормативные документы по оценке защищенных систем;
- методы и средства реализации защищенных систем;

- методы проектирования защищенных систем и систем защиты;
- системный подход к обеспечению информационной безопасности;
- технические каналы утечки информации и их свойства;
- методы организации деятельности подразделений обеспечения информационной безопасности;
- инженерно-технические средства защиты информации;
- технологические меры поддержания безопасности мероприятия по обеспечению режима секретности;
- задачи и законодательные основы организации деятельности органов, обеспечивающих информационную безопасность;
- правовые нормы и документы по информационной безопасности;
- методы защиты интеллектуальной собственности и авторского права.

IV категория - специалисты, обслуживающие защищенную информационную инфраструктуру образовательной сферы – должны отвечать следующим квалификационным требованиям:

иметь представление

- об информационной безопасности РФ;
- об источниках и способах воздействия угроз на объекты информатизации;
- о системных вопросах защиты программ и данных;
- о протоколах управления ключами;
- о роли и месте организационно-правовых мер в обеспечении информационной безопасности;

знать

- угрозы и методы нарушения информационной безопасности автоматизированных систем;
- методы и средства реализации защищенных систем;
- программно-аппаратные методы и средства защиты программ и данных; ограничения доступа к файлам, к компонентам ЭВМ, привязки программного обеспечения к аппаратному окружению и физическим носителям, хранения ключевой информации, защиты программ от изучения, защиты от разрушающих программных воздействий, защиты программ от изменения и контроля целостности;
- методы применения программно-аппаратных средств при обеспечении информационной безопасности в операционных системах, СУБД, вычислительных сетях;
- технические каналы утечки информации и их свойства;
- методы и средства защиты технических средств от утечки информации по этим каналам;
- основные мероприятия по обеспечению режима секретности;
- основные классы шифров и типовые криптографические протоколы.

Система дистанционного обучения и тестирования по вопросам информационной безопасности

В соответствии с принятой концепцией развития системы дистанционного обучения в СПбГУ ИТМО разработанный программно-методический комплекс компьютерного тестирования по вопросам информационной безопасности основан на сетевой Internet-технологии и предназначен для проведения обучения и аттестации в компьютерных IP-сетях любого масштаба [2]. Перечислим темы, включенные в комплекс.

1. Основы информационной безопасности.

Цель курса – знакомство с основными понятиями в области защиты информации; определение сущности, целей, задач и значения защиты информации; установление критериев, условий и принципов отнесения информации к защищаемой и классификация ее по собственникам, видам тайны и материальным носителям; классификация угроз безопасности информации, их причин, условий проявления, методов реализации; определение и классификация объектов, видов, методов и средств защиты информации.

2. Правовое обеспечение информационной безопасности.

Цель курса – знакомство с методами правовой защиты информации; изучение правовых основ защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных данных; изучение правовой ответственности за утечку информации и утрату носителей информации; изучение основных законодательных актов, правовых норм и положений.

3. Организационное обеспечение информационной безопасности.

Цель курса – получение представления об организационной структуре образовательного предприятия как объекта информатизации; знакомство с угрозами информационной безопасности; изучение организации службы безопасности предприятия; знакомство с методами организационной защиты информации; изучение правил засекречивания и рассекречивания конфиденциальной информации, а также допуска к такой информации; получение знаний об основных организационных мероприятиях на предприятии по предотвращению утечки конфиденциальной информации.

4. Защита государственных интересов и система сохранения государственной тайны.

Цель курса – определение и демонстрация структуры системы сохранения государственной тайны; знакомство с методами организации информационной безопасности и защиты государственных интересов; знакомство с классификацией и перечнем сведений, содержащих государственную тайну; регламентирование доступа и допуска к секретной информации; изучение контроля и надзора за сохранением режима государственной тайны.

5. Организация и управление службой защиты информации на предприятии.

Цель курса – получение представления об организационной структуре малого и среднего предприятия как объекта информации; знакомство с основными угрозами информационной безопасности на предприятии; получение представления об организации службы безопасности предприятия; изучение правил ситуационного управления защитой информации при ее обработке, хранении и передаче; получение знаний об основных организационных мероприятиях на предприятии и оптимизации контроля защищенности информации.

6. Технология сертификации средств защиты и лицензирование деятельности в области информационной безопасности.

Цель курса – раскрытие сущности, целей и задач сертификации средств защиты и лицензирования деятельности в области информационной безопасности; определение принципов и этапов сертификации средств защиты и лицензирования деятельности в области информационной безопасности; освоение технологий сертификации средств защиты и лицензирования деятельности в области информационной безопасности; овладение методами сертификационных испытаний средств защиты информации; получение умений по установлению состава и содержания мероприятий по сертификации средств защиты и лицензированию деятельности в области информационной безопасности

7. Документоведение и делопроизводство.

Цель курса – знакомство с особенностями развития государственного делопроизводства; нормативно-методической базой и основными понятиями документоведения; изучение правил работы с документами; приобретение знаний в области информационных технологии обеспечения управленческой деятельности, включая компьютерные технологии подготовки текстовых и табличных документов.

8. Защищенный документооборот.

Цель курса – изучение законодательных и нормативных актов по защите информации; знакомство с правовым полем и мерой ответственности по применению нормативных документов; изучение основ технологии защищенного документооборота; знакомство с современными носителями информации и методами её обработки; обеспечение режима при обработке информации ограниченного распространения.

9. Инженерно-техническая защита информации.

Цель курса – знакомство специалистов образовательной сферы с современными концепциями организации защиты информации техническими средствами; изучение угроз безопасности информации, обсуждение основных принципов её добывания и обработки с помощью технических средств и противодействие им.

10. Защита интеллектуальной собственности.

Цель курса – знакомство с основными понятиями патентного дела; умение ориентироваться в патентной литературе; грамотно анализировать технические решения, с целью определения их охраноспособности; проводить технико-экономические сравнения технических решений; оформлять заявки на патент, товарные знаки и промышленные образцы; грамотно защищать интеллектуальную собственность, представляемого ими юридического лица; осуществлять поиск требуемой патентной информации в Интернете.

11. Безопасность в компьютерных системах.

Цель курса – знакомство с требованиями к защите информации в компьютерных системах; изучение методов построения и анализа защиты компьютерных систем, профилактики и противодействия внешним угрозам информации; освоение практических аспектов обеспечения защиты информации в компьютерных системах и сетях.

12. Программно-аппаратные средства обеспечения информационной безопасности.

Цель курса – знакомство с составом и требованиями к программно-аппаратной защите информации; определение параметров и требований к системам идентификации и аутентификации; изучение методов и средств разграничения доступа к информации; изучение правил управления ключами и паролями; изучение методов построения защиты программного кода и защиты от разрушающих программных воздействий.

13. Криптографические методы защиты информации.

Цель курса – формирование достаточных знаний в области теории групп, теории колец, теории полей, позволяющих использовать современный математический аппарат при использовании криптографических методов защиты информации.

Программно-методический комплекс реализован в рамках системы дистанционного обучения СПбГУ ИТМО.

Основным элементом обучения в системе является выполнение обучаемым последовательных наборов тестовых заданий по отдельным дисциплинам с предъявлением системой перед тестированием, во время тестирования, а также в зависимости от результатов тестирования информационных материалов (опорных конспектов, ссылок на литературные и другие источники и т.п.).

В режиме аттестации система предназначена для проведения контроля знаний обучаемых без возможности получения подсказок, информационных материалов и т.п. В этом режиме доступ к системе осуществляется каждый раз по разрешению преподавателя, с идентификацией личности. Результаты тестирования подтверждаются деканатом и принимаются как официальная оценка. Они заносятся в базу данных как информация о выполнении учебного плана [3].

Заключение

Результаты работы использованы для создания основы системы повышения квалификации специалистов образовательной сферы по информационной безопасности, а также для обучения студентов по специальностям с квалификацией "специалист по защите информации "

Литература

1. Итоговый отчет по Государственному контракту от 11.07.2002 № 640 "Разработка концепции и образовательных программ по вопросам информационной безопасности ", СПб ГИТМО(ТУ), 2002.
2. Лисицина Л.С., Лямин А.В., Чежин М.С. Руководство пользователя компьютерной сетевой системой для проведения обучения и аттестации. СПб, ИТМО(ТУ), 2002. 43 с.
3. Техническое руководство по разработке пакетов тестовых заданий для системы дистанционного обучения СПб ГИТМО(ТУ), Центр дистанционного обучения СПб ГИТМО(ТУ), 2001.