4. Инновационные педагогические технологии : модульное пособие для преподавателей профессиональной школы / под ред. Е. В. Иванова, Л. И. Косовой, Т. Ю. Аветовой. – Санкт-Петербург : Полиграф-С, 2004. – 160 с.

5. Карташевский, В. Г. Реализация инновационных подходов в образовательном процессе при изучении инфокоммуникационных дисциплин / В. Г. Карташевский, М. А. Буранова, Н. В. Киреева // Новые информационные технологии в образовании и науке : материалы X международной научно-практической конференции. – Екатеринбург, 2017. – С. 478–483.

6. Зубова, Н. В. Реализация комплексной кейс-технологии в вузе при изучении темы «Электромагнетизм» / Н. В. Зубова // Профессиональное образование. – 2014. – № 8. – С. 170–176.

УДК [37.016:004.056]:[371.1:004]

Киреева Н. В., Поздняк И. С.

МЕТОДИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОБУЧЕНИИ УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Наталья Валерьевна Киреева
кандидат технических наук, доцент
kireeva@psuti.ru
Ирина Сергеевна Поздняк
кандидат технических наук
i.pozdnyak@psuti.ru
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Россия, Самара

METHODICAL ASPECTS OF THE USE OF INFORMATION TECHNOLOGIES IN LEARNING INFORMATION SECURITY MANAGEMENT

Natalya Valeryevna Kireeva

Irina Sergeevna Pozdnyak

Povolzhskiy State University of Telecommunication and Informatics, Russia, Samara

Аннотация*. Авторы представляют методику обучения управлению информационной безопасностью с помощью различных информационных технологий: экспертных систем и интернет-ресурсов, а также их особенности в современной концепции изучения основ управления информационной безопасностью.*

Abstract*. The authors present the methodology of information security management training using various information technologies: expert systems and Internet resources, as well as their features in the modern concept of studying the basics of information security management.*

Ключевые слова*: управление информационной безопасностью, информационные технологии, экспертные системы, интернет-ресурсы.*

Keywords*: information security management, information technology, expert systems.*

Вопросы управления информационной безопасностью (ИБ) являются актуальными в настоящее время, так как данный процесс очень трудоемок как в обучении, так и при практической реализации. Он затрагивает большой пласт вопросов, связанных с организационными мерами, реализуемыми в информационных системах предприятий различного типа и размера.

Система управления информационной безопасностью является частью комплексной системы управления, основанной на оценке и анализов рисков, для разработки, реализации, администрирования, мониторинга, анализа, под-

держания и повышения информационной безопасности (далее — ИБ) и ее реализации, полученных из целей организации и требования, требования безопасности, используемых процедур и размерах и структуре ее организации [2].

В целях облегчения понимания и восприятия материала, направленного на обучение управлением информационной безопасностью, следует применять различные информационные технологии, которые являются ключевыми инструментами. К ним относятся: презентационные материалы, глобальная сеть Интернет, экспертные системы.

Экспертные системы (ЭС) — наиболее типичная реализация искусственного интеллекта — сегодня используются в различных областях. Важной особенностью ЭС является их способность к самообучению, которая связана с непрерывным процессом обнаружения знаний и интеллектуальным анализом данных [3]. По мнению специалистов, в недалекой перспективе экспертные системы будут играть ведущую роль во всех фазах проектирования, разработки, производства, распределения, продажи, поддержки и оказания услуг. Их технология, получив коммерческое распространение, обеспечит революционный прорыв в интеграции приложений из готовых интеллектуально-взаимодействующих модулей.

В связи с динамическим развитием информационных технологий и широким применением информационных систем различной архитектуры и сложности в деятельности современных малых предприятий, существует проблема комплексной оценки системы обеспечения информационной безопасности. При этом, зачастую, для решения данной проблемы необходима команда специалистов. В рамках процесса управления информационной безопасностью (ИБ) применение экспертной системы является необходимым условием. Для этого существует несколько причин:

- возможность принятия субъективного решения, присущая человеку, сведена к нулю;
- появляется возможность разделения одной крупной задачи на несколько подзадач;

- использование человека-эксперта проблематично и дорого (особенно на малых предприятиях), а использование ЭС позволяет сократить количество специалистов и экспертов для анализа и оценки ИБ;
- сложность управления ИБ приводит к тому, что человеку необходимо много времени для того, чтобы достичь уровня эксперта.

Поэтому изучение принципов работы таких систем является необходимым условием для успешного обучения специалистов.

В процессе изучения экспертных систем студенты учатся не только работать с программными реализациями, но также подготавливать и анализировать данные, необходимые для ввода в систему.

Еще одной ключевой информационной технологией является сеть Интернет. Точнее, некоторые ее ресурсы в виде IT-сообществ. Одним из таких является Center for Internet Security (CIS) — Центр интернет-безопасности [1]. Это некоммерческая организация, которая использует возможности мирового ИТ-сообщества для защиты частных и общественных организаций от киберугроз. В его распоряжении есть множество инструментов, в том числе и для управления информационной безопасностью. Ниже рассмотрим некоторые из них.

CIS Controls и CIS Benchmarks являются всеобщим стандартом и признанными лучшими упражнениями для защиты IT-систем и данных от самых распространенных атак. Эти проверенные руководящие принципы постоянно совершенствуются и проверяются добровольным глобальным сообществом опытных IT-специалистов.

CIS Controls — это приоритетный набор действий, которые в совокупности образуют комплекс глубокой защиты. Они смягчают наиболее распространенные атаки на системы и сети. CIS Controls разрабатываются сообществом ИТ-экспертов, которые применяют свой непосредственный опыт, чтобы создать эти всемирно признанные лучшие правила безопасности.

CIS Controls основаны на фактических атаках и эффективных средствах защиты и объединяют знания экспертов: из различных частей общества (компаний, правительственных структур, отдельных лиц); различных профессий (аналитики, технологи, производители инструментов, поставщики решений, защитники, пользователи, политики, аудиторы и т. д.); из многих секторов (правительство, энергетика, оборона, финансы, транспорт, академия, консалтинг, безопасность, ИТ). Они объединились для создания, принятия и поддержки средств управления. Это гарантирует, что средства CIS Controls являются наиболее эффективным и конкретным набором технических мер, доступных для обнаружения, предотвращения, реагирования.

Для того, чтобы грамотно работать с данным документом, необходимо изучить его структуру. Кроме того, есть возможность кратко и тезисно изучить представленные средства с помощью сайта Центра интернет-безопасности CIS [1]. В общем виде CIS Controls представляет собой 20 рекомендаций по управлению ИБ, с их описанием.

В условиях ограниченности по времени при изучении основ управления информационной безопасностью рекомендуется пользоваться интернет-ресурсом [1]. В нем тезисно указаны основные особенности каждой меры безопасности, кратко перечислены основные выводы. Основным преимуществом данного ресурса является то, что помимо описания каждой рекомендации присутствует небольшая презентация, которая наглядно демонстрирует для чего нужна и как пользоваться каждой, из представленных рекомендаций. Эта отличительная особенность позволяет обучающимся в кратчайшее время получить представление обо всех рассматриваемых мерах управления ИБ.

Если в процессе обучения временные рамки не являются ограничением, то помимо интернет-ресурса следует также изучить документ, который детально рассматривает 20 мер управления информационной безопасностью. Получить этот документ можно, зарегистрировавшись на сайте Center for Internet Security. В описании каждой рекомендации присутствуют следующие

структурные элементы: описание важности меры, таблица конкретных действий, процедуры и инструменты, схемы применения. Следует также отметить, что все меры делятся на три блока: базовые, основополагающие и организационные. Это является несомненным удобством при изучении, так как появляется понимание значимости данных мер.

Другим инструментом управления ИБ, представленным ресурсом [1], являются рекомендации CIS Benchmarks. Они представляют собой набор правил по настройки систем безопасности для различных технологий и разрабатываются профессионалами в области кибербезопасности со всего мира. Эти руководящие принципы написаны более чем для 140 технологий в различных категориях: операционные системы, программное обеспечение для серверов, облачных технологий, мобильных устройств, сетевых устройств, программное обеспечение рабочих станций. В каждой из этих категорий рассмотрены наиболее часто используемые технологии. Деление на категории также очень удобно при изучении рекомендаций.

После детального изучения CIS Controls и CIS Benchmarks, в случае необходимости, можно перейти к изучению инструмента оценки конфигурации CIS — CIS-CAT (CIS Configuration Assessment Tool), который предоставляет специалистам в области информационных технологий и безопасности быструю и детальную оценку соответствия заданных систем стандартам CIS. Приложение сканирует конфигурацию выбранной системы (технологии) в режиме реального времени.

Представленные виды информационных технологий дают возможность изучения некоторых основ управления ИБ.

Необходимо отметить, что с расширением сферы использования информационных систем и их усложнением обостряется проблема обеспечения информационной безопасности, которую уже невозможно обеспечить одним лишь набором технических средств и поддерживать только силами подразделений безопасности. Данные задачи решаются путем построения эффективной

системы управления информационной безопасностью, что невозможно без понимания основ управления информационной безопасностью, методики ее организации и современных информационных технологий.

Список литературы

1. CIS Center for Internet Security [Электронный ресурс]. – Режим доступа: http:// www.cisecurity.org.

2. Гребенников, В. Управление информационной безопасностью. Стандарты СУИБ [Электронный ресурс] / В. Гребенников. – Режим доступа: http:// https://ridero.ru/books/upravlenie_informacionnoi_bezopasnostyu/#freeText.

3. Евсюков, В. В. Интеллектуальный анализ данных как инструмент поддержки принятия решений в системе банковского финансового менеджмента / В. В. Евсюков // Известия Тульского государственного университета. Экономические и юридические науки. – 2014. – № 4. – С. 374–384.

УДК [378.011.33:004]:[378.14:004]

Колесникова Ю. А., Окуловская А. Г.

ФОРМИРОВАНИЕ ИНФОРМАЦИОННОЙ КОМПЕТЕНТНОСТИ БАКАЛАВРОВ ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБРАЗОВАНИЯ

Юлия Алексеевна Колесникова

ст. преподаватель

wmmw@inbox.ru

Анастасия Георгиевна Окуловская

ст. преподаватель

okanastasiya@ya.ru

Российский государственный профессионально-педагогический университет