7. Косолапов, А. Н. Проблемы взаимосвязи информационно-образовательной среды вуза и новых информационных технологий [Электронный ресурс] / А. Н. Косолапов. – Режим доступа: http://mstu.edu.rn/publish/conf71 lntk/section4/index. html.

УДК 378.011.33:[006.44:331.543]

Карташевский В. Г., Буранова М. А., Киреева Н. В.

ИННОВАЦИОННЫЕ МЕТОДЫ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ ПО НАПРАВЛЕНИЮ УГС 10.00.00 ПРИ ПЕРЕХОДЕ НА ФЕДЕРАЛЬНЫЕ ГОСУДАРСТВЕННЫЕ ОБРАЗОВАТЕЛЬНЫЕ СТАНДАРТЫ С УЧЕТОМ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ

Вячеслав Григорьевич Карташевский
доктор технических наук, профессор
kartashevsky-vg@psuti.ru
Марина Анатольевна Буранова
кандидат педагогических наук, доцент
buranova-ma@psuti.ru
Наталья Валерьевна Киреева
кандидат педагогических наук, доцент
kireeva@psuti.ru
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Россия, г. Самара

INNOVATIVE METHODS IN THE EDUCATIONAL PROCESS BY DIRECTION OF EGS 10.00.00 AT TRANSITION TO FEDERAL STATE EDUCATIONAL STANDARDS TAKING INTO ACCOUNT PROFESSIONAL STANDARDS

Vyacheslav Grigorievich Kartashevskiy

Marina Anatolievna Buranova

Natalia Valerievna Kireeva

Povolzhskiy State University of Telecommunications and Informatics, Russia, Samara

Аннотация. *В работе рассмотрены новые образовательные технологии, позволяющие привить необходимые навыки студентам направлений подготовки по информационной безопасности. Предложен кейс-метод в рамках дисциплины, изучающей комплексные системы защиты информации на предприятии.*

Abstract*. The paper discusses new educational technologies that allow imparting the necessary skills to students in areas of information security training. A case method is proposed in the framework of the discipline that studies integrated information security systems in an enterprise*

Ключевые слова: *образовательные технологии, кейс-метод, комплексная система защиты информации, уровень защищенности.*

Keywords: *educational technologies, case method, integrated information security system, level of security.*

На сегодняшний день одной из важнейших задач, решаемых в ВУЗах, является разработка образовательных программ в соответствии с федеральными государственными образовательными стандартами с учетом профессиональных стандартов (ФГОС ВО 3++). Профстандарты направлены на выполнение следующих функций [1]:

- определить трудовой функционал работника;

- разработать ФГОСы для профессионального образования;
- создать программы профессионального обучения;
- провести независимую оценку квалификации.

Хорошо известно, что инфокоммуникационная сфера одна их наиболее активно развивающихся. При этом развитие инфокоммуникаций неразрывно связано с проблемой обеспечения информационной безопасности. Подготовка специалистов в данной сфере весьма специфична и связана с необходимостью привития выпускникам навыков, определяемых широким набором требуемых знаний в таких областях как инфокоммуникации, вычислительная техника, управление, законодательство и многих других. Образовательные стандарты и профстандарты предъявляют к специалистам данной сферы достаточно высокие требования.

При этом высокая интенсивность развития инфокоммуникационных технологий и, как следствие, средств информационной защиты требует внедрения новых инновационных образовательных технологий. Одной из возникающих проблем является трудность перехода от теории к практике, а конкретно это привитие у студентов определенных профессиональных навыков, навыков применения полученных знаний при решении практических задач.

В информационной безопасности важным является комплексность подхода к защите информации. На современном этапе сохраняется проблема разработки и внедрения комплексных систем защиты на предприятии, поскольку они включают в себя весьма широкий круг задач, связанных с законодательной базов, организационными вопросами, техническим обеспечением, администрированием и многими другими вопросами. При построении любой системы необходимо определить принципы, в соответствии с которыми она будет построена. Комплексная система защиты информации (КСЗИ) — сложная система, функционирующая, как правило, в условиях неопределенности, требующая значительных материальных затрат [2]. Для лучшего освоения материала необходимы новые подходы.

В рамках реализации основной образовательной программы (ООП) по направлениям подготовки информационная безопасность предусмотрен курс Комплексная система защиты информации.

Реформирование экономики в принципе породило существенный спрос на специалистов, умеющих действовать в ситуациях неопределённости, высокой степени риска, специалистов, умеющих анализировать и принимать решения. В ВУЗах началось массовое обновление преподаваемых дисциплин и курсов, появление большого числа интерактивных методов обучения.

В педагогической практике наиболее широко используются следующие технологии, активизирующие учебный процесс [3]:

- метод ситуационного анализа: ситуационные задачи, ситуационные упражнения;
- анализ конкретных ситуаций, кейс-стадии;
- метод ситуационно-ролевых игр;
- метод дискуссии.

Использование метода кейсов в обучении студентов позволит:

- повысить познавательный интерес к изучаемым дисциплинам;
- улучшить понимание экономических законов;
- развить исследовательские коммуникативные и творческие навыки принятия решений в проблемной ситуации на основе фактов из реальной жизни;
- сформировать конкурентоспособность, персональную и коллективную ответственность.

В рамках реализации кейс-метода на практических занятиях по КСЗИ рассмотрим два задания: первое — определение организационной структуры автоматизированной системы (АС) одного из подразделений предприятия, второе — определение организационной структуры государственной информационной системы с точки зрения обеспечения информационной безопасности заключается в определении класса защищенности государственной информационной системы (ГИС) и составлении акта классификации ГИС.

В алгоритме работы с кейсом выделяются шесть этапов.

1. Введение в проблему. Предполагает краткое описание ситуации и краткое изложение сути проблемы (желательно в одном предложении).

2. Сбор информации. Требует описания всех существенных лиц, вовлеченных в ситуацию, сопоставления аспектов, которые важны при решении обсуждаемой проблемы, поиска и оценки информации.

3. Рассмотрение альтернатив. Необходима разработка различных решений и изучение их альтернативных вариантов.

4. Принятие решения. Предполагает оценку вариантов решения проблемы и выбор оптимального решения.

5. Презентация решения. Предполагает презентацию решения и аргументацию выбора.

6. Сравнительный анализ. Включает разбор хода поиска решений, сравнение начальных и промежуточных вариантов с фактически принятым решением и анализ плана мероприятий по его реализации [4].

Данный алгоритм можно обобщить, и тогда получим кейс-метод, аналогичный показанному в [4, 5, 6], который включает три этапа: подготовительный (введение в проблему и сбор информации), основной (рассмотрение альтернатив, принятие решения) и заключительный (презентация решения, сравнительный анализ).

Подготовительный этап. Знакомство с содержимым кейса, формирование умений работать с учебной, научно-технической литературой, первичный анализ сформулированной проблемы, формирование интереса к деятельности по решению ситуационной задачи.

Первое задание — определению организационной структуры автоматизированной системы (АС) одного из подразделений предприятия, необходимо определить характер функционирования предприятия: количество рабочих мест пользователей, наличие сетевого оборудования, возможность выхода в глобальную сеть; кроме того, обрабатывается ли в сети общедоступная информация и сведения конфиденциального характера с грифом «Для служебного

пользования»; имеется ли подключение АС к сетям общего пользования и (или) сетям международного информационного обмена не имеется; является ли АС по режиму обработки информации ограниченного доступа многопользовательской; определение режима разграничения прав доступа пользователей к информации, обрабатываемой в АС.

Группа делится на несколько подгрупп в зависимости от численности, каждая из которых рассматривает свой тип предприятия. Кейс содержит необходимую литературу и возможные типы предприятий.

В результате у студентов должно сформироваться осознание значимости выбранной профессии, понимание структуры и характера взаимоотношений в области информационной безопасности.

Основной этап. определение и корректировка уровня знаний и умений в области информационной безопасности, поэтапная формировка умений по решению конкретной ситуационной задачи.

На данном этапе определяется конкретная топология сети, состав автоматизированных рабочих мест (АРМ) пользователей, серверов, коммутационного оборудования. Например, определяется необходимость выделения АРМ, принтера и сервера в отдельный логический сегмент локальной сети (VLAN — Virtual Local Area Network), отделенный от других сегментов корпоративной сети организации межсетевым экраном, особенности расположения коммуникационного оборудования.

Затем определяется технология обработки информации ограниченного доступа: допущенные к работе на АРМ сотрудники, список сотрудников, имеющих полный доступ к информации, определение других разграничений доступа для сотрудников.

Составляются распорядительные акты по разграничению доступа: устанавливается роль, уровень доступа к информации ограниченного доступа, разрешенные действия с информацией ограниченного доступа; определяются способы разграничения и управления доступа.

Далее необходимо определить Технологическую информацию, циркулирующую в АС:

- управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- общедоступная справочная информация;
- служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Информация ограниченного доступа.

Заключительный этап. Подведение итогов решения конкретной задачи. В результате студенты могут оценить значимость будущей профессии, получить адекватную самооценку, увидеть пробелы в знаниях, получить навыки самостоятельной организации и проведения проектной деятельности.

Необходимо сделать вывод о степени защищенности предприятия, для чего определяются: компоненты АС, программные средства обработки информации ограниченного доступа, установленные средства защиты.

Второе задание — определение организационной структуры государственной информационной системы с точки зрения обеспечения информационной безопасности заключается в определении класса защищенности ГИС и составлении акта классификации ГИС.

Аналогично первому заданию на подготовительном этапе студенты выбирают самостоятельно предприятие, включающее ГИС, определяют его структуру (в том числе перечень должностных лиц) и приводят краткое описание. Затем определяют перечень предоставляемых услуг. Для чего они должны изучить характер и функции подобных систем. Например, доступ физических и юридических лиц к сведениям о государственных и муниципальных услугах; предоставление в электронной форме государственных и муниципальных услуг; учет обращений граждан, связанных с функционированием Единого портала и других возможные функции.

На основном этапе определяется входит ли ГИС в инфраструктуру, обеспечивающую информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме. Кто является оператором ГИС и на основании чего, например, по решению Правительства РФ является Министерство связи и массовых коммуникаций Российской Федерации.

После чего необходимо определить способ доступа пользователей в систему и аутентификацию, например, через «личный кабинет» и с помощью логина и пароля, либо посредством электронной подписи, и способ защиты информации, установить ответственность за нарушение защищенности информации.

На заключительном этапе определяют класс защищенности ГИС и составляют акт классификации ГИС. Образец бланка акта студентам предоставляется.

Применение кейс-метода позволит сформировать у студентов навыки работы с литературой, информационными системами, получить профессиональные навыки в будущей профессии, погрузиться в реальную профессиональную практическую деятельность.

Список литературы

1. Профстандарты: какого уровня образования достаточно для продолжения работы? [Электронный ресурс]. – Режим доступа: https://academy-prof.ru/blog/profstandarty-v-obrazovani.

2. Грибунин, В. Г. Комплексная система защиты информации на предприятии : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – Москва : Академия, 2009. – 416 с.

3. Эктов, А. В. Использование Кейс метода в образовательном процессе [Электронный ресурс] / А. В. Эктов // Научно-методический электронный журнал «Концепт». – 2013. – Т. 3. – С. 416–420. – Режим доступа: http://e-koncept.ru/2013/53085.htm.

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