УДК 004.048 ♦ ВАК 05.13.01
DOI: http://dx.doi.org/10.21686/1818-4243-2018-6-59-64

В.А. Сизов
Российский экономический университет им. Г.В. Плеханова, Москва, Россия

Применение деловых игр в подготовке магистров по программе «Защита информационного пространства субъектов экономической деятельности»

Целью исследования *является разработка концепции применения деловых игр в магистерской программе по направлению подготовки «Информационная безопасность» с позиции практического обучения методам и средствам защиты информационного пространства предприятий и организаций, а также других субъектов экономической деятельности.*
Материалы и методы. *В основе разработки концепции применения деловых игр в подготовке магистров по направлению подготовки «Информационная безопасность» лежат Федеральный государственный образовательный стандарт и профессиональный стандарт «Специалист по защите информации в автоматизированных системах». В концепции проведения деловой игры определяются требования к конкретизации регламентов взаимодействия участников (акторов) информационно-образовательного пространства в соответствии с их ролевыми особенностями с учетом реализации на организационном уровне стека интероперабельности EIF (European Interoperability Framework)*
Результаты. *В статье представлена концепция применения деловых игр в подготовке магистров по программе «Защита информационного пространства субъектов экономической деятельности», обоснована необходимость использования деловых игр для конкретных дисциплин программы, предложен подход к реализации деловых игр в учебном процессе на основе взаимодействия ключевых акторов информационно-образовательного пространства, построенного на основе технологий виртуализации.*
Заключение. *Использование деловых игр в учебном процессе магистров по программе «Защита информационного пространства субъектов экономической деятельности» способствует формированию необходимых профессиональных компетенций с учетом особенностей компонентов информационного пространства субъектов экономической деятельности: информационных ресурсов, средств информационного взаимодействия и информационной инфраструктуры.*

Ключевые слова: *информационная безопасность, субъект экономической деятельности, деловая игра, информационно-образовательное пространство (ИОП), технология виртуализации*

Valeriy A. Sizov
Plekhanov Russian University of Economics, Moscow, Russia

The use of business games in the education of masters in the program “Protection of information space of economic activity”

The aim *of the study is to develop the concept of the use of business games in the master’s program in the direction of “Information security” from the perspective of practical training methods and means of protection of information space of enterprises and organizations, as well as other economic subjects.*
Materials and methods. *The basis for the development of the concept of the use of business games in the education of masters in the direction of “Information security” are the Federal state educational standard and professional standard “Specialist in the protection of information in automated systems.” The concept of the business game defines the requirements for the specification of the rules of interaction of participants (actors) of the information and educational space in accordance with their role features, taking into account the implementation at the organizational level of the EIF (European Interoperability Framework).*
Results. *The article presents the concept of using business games in preparing masters for the program “Protecting the Information Space of Economic Actors”, substantiates the need to use business games for specific disciplines of the program, proposes an approach to implementing business games in the educational process based on the interaction of key actors in the information and educational space built on the basis of virtualization technologies.*
Conclusion. *The use of business games in the educational process of masters in the program “Protection of the information space of economic activity” contributes to the formation of the necessary professional competencies, taking into account the features of the components of the information space of economic activity: information resources, means of information interaction and information infrastructure.*

Keywords: *information security, subject of economic activity, business game, information and educational space (IEP), virtualization technology*

Введение

Информационная революция, начавшаяся в конце 20 века, привела к появлению новых ресурсов, групп пользователей и их взаимодействий, обусловила новый технологический уклад экономики и одновременно вскрыла проблемы развития цифровой экономики, одной из которых является проблема информационной безопасности. В доктрине информационной безопасности Российской Федерации указано, что защита информационного пространства является одним из приоритетов

обеспечения национальной безопасности РФ [1]. В настоящее время очевидно, что решение этой проблемы связано с совершенствованием подготовки кадров в новых сферах профессиональной деятельности: экономической и финансовой безопасности; аналитики в области информационной безопасности; деловой разведки; юриспруденции в сфере компьютерной безопасности, комплексного обеспечения информационной безопасности субъектов экономической деятельности.

От качества подготовки кадров в этих сферах профессиональной деятельности зависит эффективность более масштабных социальных, правовых, экономических и управленческих регуляций социума.

Существенным недостатком традиционного обучения будущих бакалавров и магистров в области информационной безопасности в вузе работодатели отмечают слабую практическую ориентированность полученных знаний и компетенций. Именно поэтому для подготовки кадров в области информационной безопасности целесообразно использовать новые технологии обучения, потребностно-требовательные модели, которые могут послужить мостиком между теорией и практикой, высшим образованием и профессиональной деятельностью. Хорошо апробированной в образовании формой организации учебного процесса является деловая игра. Учебная деловая игра – это вариативная, динамично развивающаяся форма организации целенаправленного взаимодействия деятельности и общения всех участников при осуществлении педагогического руководства со стороны преподавателя [2–4]. Приобретение опыта через игровые программы происходит путем вовлечения в процесс, посредством действий, позволяющих обеспечивать нужный результат. Результативность деловых игр подтверждается следующими сведениями: прочитанное запоминается на 10%; услышанное — на 20%; увиденное — на 30%; увиденное и услышанное одновременно — на 50%; осуществленное действие — на 90% [5]. Для эффективного использования деловых игр в подготовке магистров по программе “Защита информационного пространства субъектов экономической деятельности” необходимо на компетентностном уровне определить дисциплины, для которых эта форма учебного процесса наиболее приемлема, а также обосновать структуру информационного образовательного пространства для реализации этой формы обучения.

1. Анализ программы «Защита информационного пространства субъектов экономической деятельности»

Анализ компетенций и обеспечивающих их дисциплин по направлениям подготовки в сфере информационной безопасности как на уровне бакалавриата, так и на уровне магистратуры показывает, что все они требуют формирования у обучаемых предметно-деятельностного подхода к освоению материала учебных дисциплин. Это обусловлено диалектическим противоречием «защиты/нападения», лежащим в основе развития средств защиты информации и атак на информацию в цифровой экономике. Без понимания предметно-деятельностного содержания ролей защищающегося и атакующего в условиях развития цифровой экономики невозможно глубокое и качественное освоение всего блока профессиональных дисциплин по направлениям подготовки в области информационной безопасности.

К основным профессиональным компетенциям кадров в сфере информационной безопасности можно отнести способности: к анализу угроз и уязвимостей, выявлению причинно-следственных связей между ними, защите контента, защите данных ограниченного доступа, поиску и анализу вредоносного кода и др.

В качестве примера в табл.1 представлены результаты экспертной оценки применения деловых игр для изучения дисциплин базовой и вариативной части рабочего учебного плана по программе магистратуры 10.04.01 Информационная безопасность, направленность программы «Защита информационного пространства субъектов экономической деятельности2. Эти результаты свидетельствуют о широком охвате дисциплин, для которых целесообразно использовать деловые игры (около 90%) и 50% дисциплин могут включать рефлексивные игры.

В табл.2 представлены результаты анализа компетенций магистров, прошедших обучение по программе магистратуры «Защита информационного пространства субъектов экономической деятельности», направленных на решение научно-технических проблем обеспечения информационной безопасности Российской Федерации. Таким образом содержание деловых игр, разрабатываемых для учебного процесса по программе магистратуры «Защита информационного пространства субъектов экономической деятельности» полностью согласуется с научно-техническими проблемами обеспечения информационной безопасности Российской Федерации.

2. Обоснование структуры информационного образовательного пространства для реализации

Для использования деловых игр в реализации программы “Защита информационного пространства

Таблица 1

Экспертная оценка применения деловых игр для изучения дисциплин базовой и вариативной части рабочего учебного плана по программе магистратуры 10.04.01 Информационная безопасность, направленность программы «Защита информационного пространства субъектов экономической деятельности»

№ п/п	Наименование дисциплины	Перечень формируемых компетенций	Деловые игры	Рефлексивные игры
1	Иностранный язык делового и профессионального общения	ОПК-1	+	–
2	Современные теории и механизмы управления	ОПК-1; ПК-12; ПК-13	–	+
3	Деловые и научные коммуникации	ОПК-1	+	–
4	Технологии эффективного менеджмента	ПК-12; ПК-13	+	–
5	Защищенные информационные системы	ОПК-2; ПК-1; ПК-3; ПК-6; ПК-7; ПК-8; ПК-15	+	+
6	Управление информационной безопасностью	ОПК-2; ПК-5; ПК-9; ПК-16	+	+
7	Технология обеспечения информационной безопасности	ПК-2; ПК-4; ПК-10; ПК-14	+	–
8	Теория рисков (продвинутый уровень)	ПК-5; ПК-7	+	+
9	Методология и методы исследований в области информационной безопасности	ПК-1; ПК-5; ПК-6	+	+
10	Антикоррупционные информационно-аналитические субъекта экономической деятельности	ОПК-2; ПК-1; ПК-3; ПК-7; ПК-15	+	+
11	Угрозы и риски информационной безопасности субъекта экономической деятельности	ОПК-2; ПК-1; ПК-8; ПК-12	+	+
12	Проектирование системы информационной безопасности предприятий и организаций	ПК-2; ПК-3; ПК-4	+	+
13	Мониторинг информационного пространства субъектов экономической деятельности	ОПК-2; ПК-6; ПК-12	+	–
14	Методология выявления технических каналов утечки информации	ПК-2; ПК-7; ПК-8; ПК-10	+	–
15	Информационно-психологическая безопасность	ОПК-2; ПК-1	+	+
16	Международные и российские стандарты информационной безопасности	ОПК-2; ПК-6; ПК-8	–	–
17	Консалтинг комплексной безопасности субъектов экономической деятельности	ОПК-2; ПК-6; ПК-7; ПК-8	+	+
18	Бенчмаркинг комплексной безопасности субъекта экономической деятельности	ОПК-2; ПК-6; ПК-7; ПК-8	+	–
19	Методы и инструментарий конкурентной разведки	ПК-3; ПК-8; ПК-12	+	+
20	Деловые игры в конкурентной разведке	ОПК-2; ПК-1; ПК-8; ПК-12	+	+
21	Ситуационные центры в решении задач защиты информационного пространства СУЭД	ПК-6; ПК-9	–	+
22	Информационно-аналитические системы в решении задач защиты информационного пространства субъектов экономической деятельности	ПК-6; ПК-9	+	+

Перечень общепрофессиональных и профессиональных компетенций

№ п/п	Наименование компетенции	Код
1	Способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности	ОПК-1
2	Способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности	ОПК-2
3	Способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ПК-1
4	Способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	ПК-2
5	Способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	ПК-3
6	Способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	ПК-4
7	Способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	ПК-5
8	Способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок	ПК-6

№ п/п	Наименование компетенции	Код
9	Способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	ПК-7
10	Способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ПК-8
11	Способность проводить аудит информационной безопасности информационных систем и объектов информатизации	ПК-9
12	Способность проводить аттестацию объектов информатизации по требованиям безопасности информации	ПК-10
13	Способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	ПК-12
14	Способность организовать управление информационной безопасностью	ПК-13
15	Способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	ПК-14
16	Способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	ПК-15
17	Способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности	ПК-16

Таблица 2

Взаимосвязь научно-технических проблем обеспечения информационной безопасности Российской Федерации и общепрофессиональных и профессиональных компетенций программы магистратуры 10.04.01 Информационная безопасность, направленность программы «Защита информационного пространства субъектов экономической деятельности»

N п/п	Наименование научно-технической проблемы обеспечения информационной безопасности Российской Федерации	Компетенции
1	Исследование проблем создания и развития защищенных информационно-телекоммуникационных систем, в том числе разработка методов выбора архитектуры и расчета параметров этих систем, математических моделей и технологий управления, системного и прикладного программного обеспечения с интеграцией функций защиты, средств взаимодействия, устройств передачи и распределения информации.	ОПК-1, ОПК-2, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16
2	Разработка моделей угроз безопасности систем и способов их реализации, определение критериев уязвимости и устойчивости систем к деструктивным воздействиям, разработка методов и средств мониторинга для выявления фактов применения несанкционированных информационных воздействий, разработка методологии и методического аппарата оценки ущерба от воздействия угроз информационной безопасности.	ПК-1, ПК-5, ПК-6
3	Разработка методов и средств проведения экспертизы и контроля качества защиты информации и информационных ресурсов, в том числе вопросов оценки базовых общесистемных программных средств на соответствие требованиям информационной безопасности.	ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-12, ПК-13, ПК-14, ПК-15
4	Разработка методов и средств обеспечения информационной безопасности информационных и телекоммуникационных систем, в том числе автоматизированных систем управления безопасностью, методов и средств распределения ключей и защиты информации и информационных ресурсов от несанкционированного доступа и разрушающего информационного воздействия, антивирусных технологий, методов и средств контроля состояния защищенности от НСД.	ПК-2, ПК-3, ПК-16

субъектов экономической деятельности", включающей в значительной степени неоднородные по своему деятельностному содержанию учебные дисциплины и научно-образовательные ресурсы необходимо обеспечение взаимодействия участников игры в едином информационно-образовательном пространстве (ИОП), в котором интегрируется разнородный научно-образовательный контент с использованием разнообразных программных сервисов. Ключевой задачей при создании информационно-образовательного пространства деловых игр является организация эффективного взаимодействия акторов ИОП в ходе подготовки и реализации игровых сервисов.

Выбор и проведение деловых игр осуществляется с учетом их адекватности формируемым компетенциям и оценки соответствующего уровня подготовки обучаемых и преподавателей. Для решения задачи подготовки и проведения деловой игры требуется конкре-

тизировать регламенты работы каждого актора в информационно-образовательном пространстве, определив последовательность действий акторов и общую интеграционную схему взаимодействия в ИОП на организационном уровне стека интероперабельности EIF (European Interoperability Framework, сокр. EIF) [6]. В рамках информационно-образовательного пространства можно выделить следующих акторов как ролевых субъектов образовательной деятельности: обучаемых с присвоенными ролями «защита», «нападение», менеджеров образовательных программ, менеджеров ресурсов, администратора ИОП.

Для разработки и создания универсальной информационной инфраструктуры, реализующей различные игровые сервисы целесообразно использовать технологии виртуализации. Это обусловлено наличием в большинстве вузов необходимого технического обеспечения, а также гибкостью и низкой стоимостью самих технологий виртуализации.

Информационная инфраструктура должна обеспечивать имитационное моделирование конкретных условий и динамики производственных процессов, моделирования реальных условий достижения информационной безопасности субъектов экономической деятельности; совместной деятельности всех акторов, вовлекающих в познавательную деятельность обучаемых; выбора характеристики ролей, определения их полномочий, интересов и средств деятельности с применением игровых сервисов.

Заключение

Таким образом, использование деловых игр в учебном процессе магистров по программе “Защита информационного пространства субъектов экономической деятельности” позволяет реализовать их основные достоинства для формирования необходимых профессиональных компетенций с учетом особенностей компонентов информационного пространства субъектов экономической деятельности: информационных ресурсов, средств информационного взаимодействия и информационной инфраструктуры; и обеспечивающих комплексность решения актуальных профессиональных задач защиты информационного пространства субъектов экономической деятельности.

Применение деловых игр позволяет выпускнику с одной стороны сделать его теоретическую подготовку в области методологических основ защиты информационного пространства субъектов экономической деятельности транспарентной в условиях развития цифровой экономики, а с другой – приобрести необходимые практические навыки по использованию современных инструментальных средств для решения поставленных профессиональных задач.

Литература

1. Доктрина информационной безопасности Российской Федерации. Дата подписания 5 декабря 2016 г.

2. Наумова Т.Н. Применение деловых игр в управлении персоналом сервисных предприятий // Научное сообщество студентов XXI столетия. Экономические науки: сб. ст. по мат. XXIX междунар. студ. науч.-практ. конф. № 2(29). [Электрон. ресурс] Режим доступа: http://sibac.info/archive/economy/2(29).pdf (дата обращения: 28.12.2018)

3. Ловчева Л. В. Деловая игра как один из активных игровых методов // Концепт. 2016. Т. 23. С. 42–46. [Электрон. ресурс] Режим доступа: http://ekoncept.ru/2016/56389.htm.

4. Сизов В.А. Методология разработки моделей системы информационного противоборства // Материалы 19-й научно-практической конференции «Инжиниринг предприятий и управление знаниями». ФГБОУ ВО «РЭУ им. Г.В. Плеханова». Москва, 2016.

5. Электронный журнал: деловые игры [Электрон. ресурс] Режим доступа http://www.businessgames.ru/

6. Тельнов Ю.Ф. Модель многоагентной системы реализации информационно-образовательного пространства // Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014 (24–27 сентября 2014 г., Казань, Россия): Труды конференции. Т.1. Казань: Изд-во РИЦ «Школа», 2014.

7. ITIL 2011, Service Design, TCO.

References

1. The doctrine of information security of the Russian Federation. December 5, 2016 (In Russ.)

2. Naumova T.N. The use of business games in the management of service enterprises personnel. Nauchnoye soobshchestvo studentov XXI stoletiya. Ekonomicheskiye nauki: sb. st. po mat. XXIX mezhdunar. stud. nauch.-prakt. konf. = Scientific community of students of the XXI century. Economic Sciences: Sat. Art. mat. XXIX int. stud scientific-practical conf. № 2(29). [Internet] Available from: http://sibac.info/archive/economy/2(29).pdf (cited: 28.12.2018) (In Russ.)

3. Lovcheva L. V. Business game as one of the active game methods. Kontsept = Concept. 2016; 23: 42–46. [Internet] Available from: http://ekoncept.ru/2016/56389.htm. (In Russ.)

4. Sizov V.A. Methodology of developing models of information confrontation system. Materialy 19-y nauchno-prakticheskoy konferentsii "Inzhiniring predpriyatiy i upravleniye znaniyami" = Materials of the 19th scientific-practical conference "Engineering of enterprises and knowledge management". PRUE. Moscow; 2016. (In Russ.)

5. Elektronnyy zhurnal: delovyye igry = Electronic Journal: business games [Internet] Available from http://www.businessgames.ru/ (In Russ.)

6. Tel'nov YU.F. Model of a multi-agent system for implementing the information and educational space. Chetyrnadtsataya natsional'naya konferentsiya po iskusstvennomu intellektu s mezhdunarodnym uchastiyem KII-2014 = Fourteenth National Conference on Artificial Intelligence with International Participation KII-2014 (September 24-27, 2014, Kazan, Russia): Proceedings of the Conference. T.1. Kazan: Publishing House RIC "School"; 2014 (In Russ.)

7. ITIL 2011, Service Design, TCO

Сведения об авторе

Валерий Александрович Сизов
Д.т.н., профессор кафедры Прикладной информатики и информационной безопасности
Российский экономический университет им. Г.В. Плеханова, Москва, Россия
Эл. почта: Sizov.va@rea.ru
Тел.: +7(495)800-12-00 (д. 2023)

Information about the authors

Valeriy A. Sizov
Dr. Sci. (Engineering), Professor of the Department of Applied Informatics and Information Security
Plekhanov Russian University of Economics, Moscow, Russia
E-mail: Sizov.va@rea.ru
Tel.: +7(495)800-12-00 (д. 2023)