УДК 004.05; 004.052.3; 004.056

С. М. Авдошин, канд. техн. наук, проф.,
e-mail: savdoshin@hse.ru,
А. А. Савельева, канд. техн. наук, доц.,
Национальный исследовательский университет
"Высшая школа экономики"

Междисциплинарный подход к изучению информационной безопасности на основе анализа конкретных ситуаций[1]

Предлагается подход к преподаванию информационной безопасности, основанный на использовании метода кейс-стади для проведения практических занятий. Обосновывается целесообразность применения метода кейс-стади на примере его использования в рамках курсов "Организация и технология защиты информации" и "Технологии обеспечения информационной безопасности", читаемых студентам магистратуры и бакалавриата отделения программной инженерии НИУ "ВШЭ" с 2008 г. Данная работа восполняет отсутствие методических рекомендаций по использованию метода кейс-стади при преподавании в высших учебных заведениях дисциплин, связанных с защитой информации.

Ключевые слова: *информационная безопасность, кейс-стади, управление рисками, методические рекомендации*

Введение

Метод case study (кейс-стади, метод конкретных ситуаций) представляет собой интерактивную технологию для обучения на основе реальных или вымышленных бизнес-ситуаций, способствующую не только усвоению знаний, но и формированию у слушателей аналитических навыков и умений разрешения проблемных ситуаций. Словарь [17] описывает case study как "исследовательский проект, в котором в качестве предмета исследования выбирается единичный случай или несколько избранных примеров ... и определяется совокупность методов их изучения". Менее формальное определение предложено в работе К. Ф. Хэррайда [4]: "Case study — это история с образовательным подтекстом".

Метод конкретных ситуаций возник в начале XX века в Школе бизнеса Гарвардского университета, известной своими инновациями [13]. Распространение метода в мире началось в 70—80-е годы, тогда же метод получил известность и в СССР. Анализ ситуаций начал использоваться при обучении управленцев, в основном на экономических специальностях вузов, в первую очередь как метод обучения принятию решений. Значительный вклад в разработку и внедрение этого метода внесли Г. А. Брянский, Ю. Ю. Екатеринославский, О. В. Козлова, Ю. Д. Красовский, В. Я. Платов, Д. А. Поспелов, О. А. Овсянников, В. С. Рапоппорт и др.

Создание учебной среды, способствующей развитию навыков анализа информации, обнаружения связей между фактами и формирования гипотез, было признано особенно актуальным после публикаций западными исследователями статей о несоответствии уровня образования потребностям современного общества [3, 2, 6, 7].

Новая волна интереса к методу кейс-стади в России началась в 90-е годы в связи с ростом спроса на специалистов, умеющих действовать в ситуациях, связанных с риском или неопределенностью, анализировать проблемы и принимать обоснованные решения. Это привело к распространению практики использования метода кейс-стади в программах гуманитарных и экономических дисциплин, таких как политология, менеджмент, маркетинг, социология и т. д. (см., например, [12, 14, 15, 17]).

Одной из главных тенденций образования в области защиты информации является осознание необходимости использования принципов управления рисками при решении проблем, связанных с обеспечением информационной безопасности [1, 5]. Эта тенденция особенно ясно прослеживалась в условиях мирового финансового кризиса, так как с ростом числа "обиженных" в результате сокращений сотрудников увеличивалась вероятность совершения преступлений в отношении информационных ресурсов предприятий. Наиболее востребованными становятся специалисты по обеспечению информационной безопасности (ИБ), умеющие учитывать не только технические, но и организационные аспекты обеспечения ИБ. Это делает целесообразным применение для подготовки специалистов по защите информации метода кейс-стади, показавшего свою эффективность для развития навыков анализа

[1] Работа выполнена в рамках исследовательского проекта "Исследование и разработка методов оценки эффективности использования криптографических средств защиты информации в сфере бизнеса и финансов", поддержанного государственным грантом № П965 от 27 мая 2010 г.

ситуаций и принятия решений в условиях реального мира. Однако, как показал анализ российских и англоязычных публикаций, до сих пор отсутствуют методические разработки по использованию метода кейс-стади при преподавании в высших учебных заведениях дисциплин, связанных с защитой информации.

В данной работе предлагается подход к преподаванию информационной безопасности, основанный на использовании метода кейс-стади для проведения практических занятий. Описывается методика разработки кейс-стади по информационной безопасности и приводятся примеры, используемые при чтении курсов "Организация и технология защиты информации" и "Технологии обеспечения информационной безопасности" студентам магистратуры и бакалавриата отделения программной инженерии ГУ-ВШЭ. В заключении приводятся выводы о влиянии метода кейс-стади на ход учебного процесса и освоение студентами материалов курса, сделанные на основе опыта применения данного подхода.

Принципы использования кейс-стади

Использование метода кейс-стади позволяет увидеть неоднозначность решения проблем в реальной жизни. Цель метода кейс-стади [18] — научить студентов самостоятельно и в составе группы:

- анализировать информацию,
- сортировать ее для решения поставленной задачи,
- выявлять ключевые проблемы,
- генерировать альтернативные пути решения и оценивать их,
- выбирать оптимальное решение и формировать программы действий.

Для того чтобы учебный процесс на основе метода кейс-стади был эффективным, необходимы два условия: методика использования кейса в учебном процессе и хороший кейс. Согласно приведенным в работе [18] результатам опроса преподавателей, целью которого было выяснение основных проблем при внедрении метода кейсов (*case*) в учебный процесс, наибольшие трудности обычно вызывает *подбор подходящего кейса* и *недостаток методических разработок по использованию метода кейсов* при обучении конкретным дисциплинам. В частности, при попытке внедрить метод кейс-стади в учебную программу дисциплин по информационной безопасности мы столкнулись со следующими проблемами:

- отсутствие готовых кейсов в открытом доступе,
- невозможность использования материалов из консалтинговой практики,
- отсутствие методических рекомендаций по разработке.

В следующих разделах будет показано, как общие принципы построения и использования можно адаптировать при преподавании дисциплин, связанных с защитой информации. Мы приведем разработанные нами рекомендации по разработке кейсов по информационной безопасности, а также расскажем о выявленных нами особенностях использования кейс-стади в учебном процессе.

Структура кейс-стади

Существуют общепринятые правила построения кейс-стади. Для кейс-стади, разработанного в Гарварде, типичной чертой является сознательная перегруженность информацией. Западноевропейские школы придерживаются объема в 1—2 страницы печатного текста.

Структура кейс-стади, которой мы придерживаемся при разработке материалов для нашего курса, выглядит следующим образом.

1. Название.
2. Краткая аннотация.
3. Ключевые слова.
4. Основная часть.
5. Вопросы и задания.
6. Анализ ситуации/решение.
7. Методические указания.
8. Список использованных источников.

Для самостоятельной проработки студент получает сокращенную версию кейс-стади: разделы 1—5 и 8. Разделы 1—2 и 4—6 являются стандартными. Наличие раздела 3, на наш взгляд, серьезно облегчает процесс подбора кейса для закрепления определенной темы. Раздел 7 является руководством по использованию кейс-стади для преподавателя и не всегда публикуется в западных сборниках. В случае сложных кейсов его наличие оправдано, но зачастую для проведения практического занятия достаточно знакомства с разделом 6.

Процесс разработки кейс-стади

Основные источники идеи для сюжета кейс-стади перечислены ниже [13]:

1) информация, полученная в ходе исследовательского или консалтингового проекта или целенаправленного сбора информации;

2) воображение автора;

3) средства массовой информации, специализированные журналы и буклеты, распространяемые на выставках, презентациях и т. д.

Особенностью консалтинговых проектов, связанных с защитой информации, является обязательство исполнителя не разглашать полученные об организации-заказчике сведения (что формально закрепляется в документе под названием "Соглашение о неразглашении" — "Nondisclosure agreement", подписываемом обеими сторонами). Особенно актуальным это является для российского (традиционно закрытого) бизнеса. Таким образом, вариант (1)

для разработки кейс-стади по информационной безопасности практически неприменим.

Недостатком подхода (2) является отстраненность от реального бизнеса, что противоречит самой сути метода конкретных ситуаций.

В случае применения подхода (3) для выбора темы и сбора информации могут использоваться:

- новостные порталы по информационной безопасности (http://www.itsec.ru/, http://infosecurity.report.ru/, http://pd.rsoc.ru/ и др.);
- сайты компаний, занятых в области защиты информации (http://www.kaspersky.ru/, http://www.infowatch.ru/, http://www.securitylab.ru/news/ и др.);
- профессиональные сообщества (RISSPA — Лента инцидентов информационной безопасности http://www.linkedin.com/groups?mostPopular = &gid = 3796607, Информационная безопасность http://professionali.ru/GroupInfo/636).

Преимуществом такого подхода является то, что информация уже частично систематизирована, а недостатками — сложность получения деталей, необходимых для полноценного анализа ситуации, и субъективная оценка ситуации авторами используемых публикаций. Тем не менее, сделать историю интересной и избежать предвзятого отношения можно за счет изменения имен ключевых фигурантов и "обогащения" ситуации подробностями на основе аналогичных ситуаций.

Наиболее продуктивным, по нашему мнению, является описанный выше "комбинированный" метод, основанный на творческой переработке материала из открытой прессы с добавлением авторских деталей, позволяющих адаптировать ситуацию с учетом уровня подготовки слушателей и сделать кейс-стади целостной историей, интересной для проведения анализа.

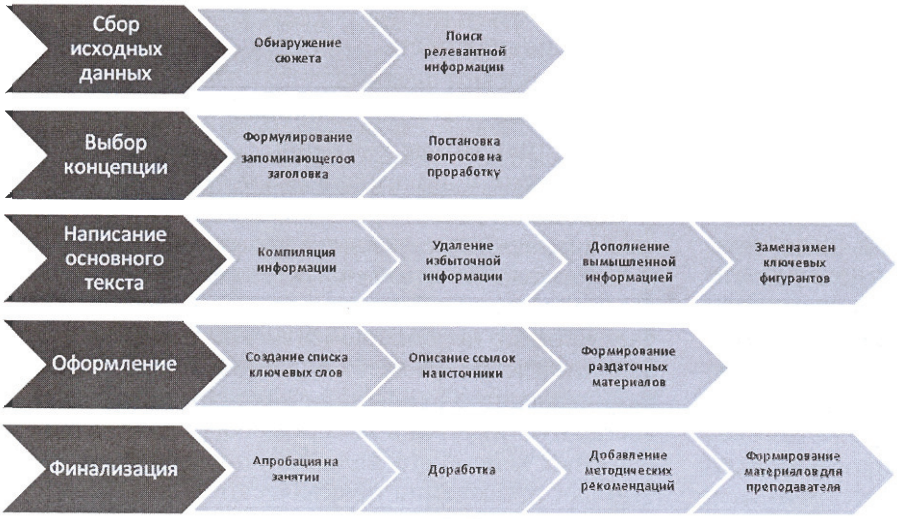

Рис. 1. Процесс создания кейс-стади

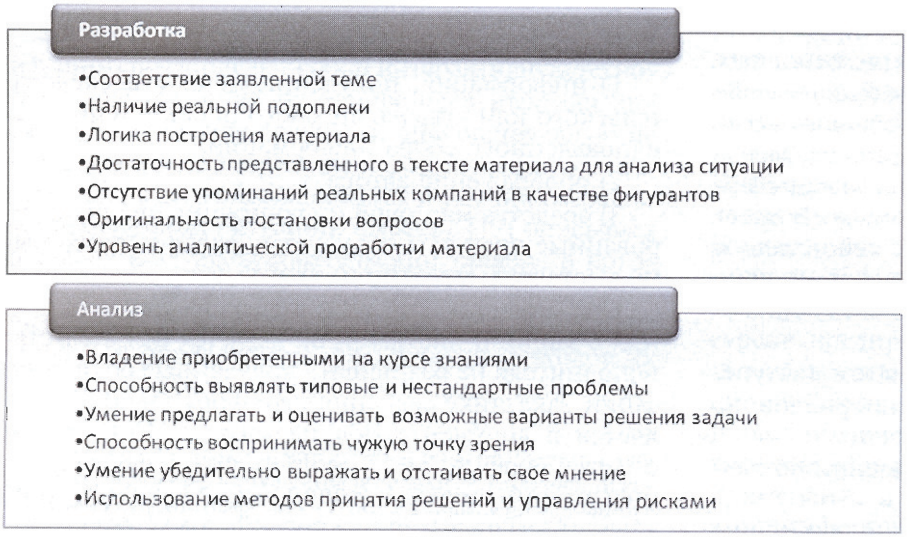

Рис. 2. Критерии оценки работы над кейс-стади

Методика использования кейс-стади в учебном процессе

Процесс создания кейс-стади представлен на рис. 1. Как правило, работа с кейс-стади строится следующим образом: преподаватель выдает текст студентам для самостоятельной проработки и затем инициирует дискуссию по вопросам, сформулированным в тексте.

На наш взгляд, эффективной является другая форма обучения, когда студенту предлагается самостоятельно подготовить кейс-стади по тематике курса. Такая форма выполнения курсовой работы была предложена студентам бакалавриата 4-го курса. При оценке работы учитывались следующие критерии:

- соответствие заявленной теме;
- логика построения материала;
- достаточность представленного в тексте материала для анализа ситуации;
- отсутствие упоминаний реальных компаний в качестве фигурантов;
- оригинальность постановки вопросов;
- уровень аналитической проработки материала;
- владение приобретенными на курсе знаниями и навыками при анализе ситуации.

Разработанные студентами кейс-стади могут быть использованы в учебном процессе, что обеспечивает постоянное пополнение банка кейс-стади. При накоплении достаточно большого числа кейс-стади мы планируем использовать этот метод при проведении экзамена как эффективный метод оценки освоения студентами пройденного материала. На рис. 2 представлены критерии оценки работы студентов с кейс-стади.

Выводы

Преимуществами подхода к преподаванию информационной безопасности, основанного на использовании метода кейс-стади, являются:

- ориентация на практические аспекты обеспечения информационной безопасности в условиях реального мира;
- высокий уровень вовлеченности студентов;
- фокусирование внимания студентов не только на технических, но и на организационных аспектах обеспечения информационной безопасности;
- демонстрация необходимости применения методов управления рисками для обеспечения защиты информации;
- возможность проведения практических занятий при минимальном уровне оснащенности аудитории;
- комплексный подход к проблеме обеспечения информационной безопасности с разных позиций — пользователя, технического специалиста, финансового директора, архитектора и топ-менеджера.

Заключение

Предлагаемый подход внедрен в учебный процесс кафедры "Управление разработкой программного обеспечения" отделения программной инженерии Государственного университета — Высшей школы экономики в рамках учебных курсов "Организация и технология защиты информации" (Магистратура; программа: Управление разработкой программного обеспечения"; 2-й курс, модуль 1, 2) и "Технологии обеспечения информационной безопасности" (Бакалавриат; специализация "Программная инженерия"; 4-й курс, модуль 3).

Апробация подхода была проведена на конференции-марафоне Training Labs'2010 в формате интерактивного тренинга "Кейс-стади: управление рисками в мире цифровых зависимостей", разработанного на основе материалов курса "Организация и технологии защиты информации".

Курс "Технологии и продукты Microsoft в обеспечении информационной безопасности", в основу которого легло использование предлагаемого подхода, на конкурсной основе получил поддержку в виде гранта "Разработка курсов по информационным технологиям", организованного компанией Microsoft (курс опубликован в библиотеке учебных курсов Центра образовательных ресурсов Microsoft [10] и в Интернет-Университете Информационных Технологий [11], где имеет высокий рейтинг популярности — 4,83 из 5 по состоянию на 19.12.2010).

Разработанная методика получила высокую оценку на Международной конференции по проблемам компьютерной безопасности "IT Security for the Next Generation — 2011" (Тур России и СНГ — 3-е место [16], Международный финал в Мюнхене — специальный приз [8]) и на семинаре "Глобальные проблемы информационной безопасности — 2011", Будапешт ("2011 Workshop on Cyber Security and Global Affairs", Budapest) [9].

На заседании Бюро Совета программы "Фонд образовательных инноваций НИУ ВШЭ" 29 июня 2011 г. по итогам весенних конкурсов образовательных инноваций работа "Методика подготовки и проведения семинарских занятий по информационной безопасности на основе изучения конкретных ситуаций" была признана победившей в номинации, посвященной разработке и внедрению в учебный процесс оригинальных методик проведения семинарских занятий, а также оригинальных методик проведения НИС в бакалавриате и магистратуре.

Список литературы

1. **Blakley B., McDermott E., Geer D.** Information security is information risk management // NSPW '01 Proceedings of the 2001 workshop on New security paradigms, ACM, 2001

2. **Brown J. S., Collins A., Duguid P.** Situated cognition and the culture of learning. Educational Researcher. 1989. Vol. 17. P. 32—42.

3. **Chipman S., Segal J., Glaser R.** Thinking and learning skills: Current research and open questions (Vol. 2). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc. 1985.

4. **Herreid C. F.** Start With a Story: The Case Method of Teaching College Science, National Science Teachers Association, 2006. 350 p.

5. **ISO/IEC** 27005:2008 Information technology — Security techniques — Information security risk management.

6. **Nickerson R. S.** On improving thinking through instruction // Review of Research in Education. 1988. Vol. 15. P. 3—57.

7. **Resnick L. B., Klopfer L. E.** Education and learning to think. Washington, DC: National Academy Press. Toward the thinking curriculum: Current cognitive research. Alexandria, VA: Association for Supervision and Curriculum Development, 1987.

8. **Savelieva A.** Special Considerations in Using the Case-study Method in Teaching Information Security // In Proceedings of 'IT Security for the Next Generation', TUM, Germany, Garching, Boltzmannstr. 3, 14—15 April 2011. URL: http://www.kaspersky.com/images/alexandra_savelieva-10-95017.pdf (дата обращения: 07.07.2011).

9. **Savelieva A. A., Avdoshin S. M.** Information Security Education and Awareness: Start with a Story // In proceedings of "2011 Workshop on Cyber Security and Global Affairs". URL: http://www.internationalcybercenter.org/workshops/cs-ga-2011/asavelieva (дата обращения: 07.07.2011).

10. **Авдошин С. М., Савельева А. А., Сердюк В. А.** Технологии и продукты Microsoft в обеспечении информационной безопасности // Библиотека учебных курсов Центра образовательных ресурсов Microsoft. 2010. URL: https://www.facultyresourcecenter.com/curriculum/pfv.aspx?ID = 8476&Login =

11. **Авдошин С. М., Савельева А. А., Сердюк В. А.** Технологии и продукты Microsoft в обеспечении информационной безопас-

ности // Интернет-Университет Информационных Технологий. 2010. URL: http://www.intuit.ru/department/security/mssec/

12. **Багиев Г. Л., Наумов В. Н.** Руководство к практическим занятиям по маркетингу с использованием кейс-метода // Энциклопедия маркетинга [Электронный ресурс]. URL: http://www.marketing.spb.ru/read/m21/

13. **Зобов А. М.** Метод изучения ситуаций (case-study) в образовании: его история и применение. Центр дистанционного образования Elitarium, 2006. URL: http://www.elitarium.ru (дата обращения: 07.07.2011).

14. **Камински Х.** Дидактико-методические основы преподавания экономики. Изучение конкретного случая (case-study) // Экономика. Вопросы школьного экономического образования. 1998. № 2.

15. **Парамонова Т. Н., Блинов А. О., Шереметьева Е. Н., Погодина Г. В.** Маркетинг: активные методы обучения. М.: КНОРУС, 2009.

16. **Савельева А. А.** Особенности использования метода case-study при преподавании информационной безопасности // Сб. тр. Международной студенческой конференции по проблемам компьютерной безопасности "IT-Security Conference for the Next Generation", 9—11 марта 2011 г., г. Москва, факультет Вычислительной математики и кибернетики Московского государственного университета [Электронный ресурс]. URL: http://www.kasperskyacademy.com/ru/view.html?id = 392 (дата обращения: 07.07.2011).

17. **Социология**: Энциклопедия / Сост. А. А. Грицанов, В. Л. Абушенко, Г. М. Евелькин, Г. Н. Соколова, О. В. Терещенко. Минск: Интерпрессервис; Книжный Дом, 2003. 1312 с. (Сер. Мир энциклопедий).

18. **Шумилова Ю. А.** Использование метода кейс-стади при преподавании маркетинговых дисциплин // Проблемы и перспективы управления экономикой и маркетингом в организации, Тюмень: Тюменский государственный университет, 2009. № 9.










IV международная конференция

"Проблемы кибернетики и информатики" (PCI'2012)

12—14 сентября 2012 г., Баку, Азербайджан

Научная тематика конференции

- информационные и коммуникационные технологии
- интеллектуальные технологии и системы
- сейсмические приборы, системы и технологии
- моделирование и идентификация
- численные методы и вычислительные технологии
- прикладной стохастический анализ
- управление и оптимизация
- принятие решений в социально-экономических системах

Доклады

Доклады представляются на английском языке объемом не более 4 страниц. Требования для оформления докладов размещены на *www.pci2012.science.az*

Финансовые вопросы

Организационные взносы участников конференции, а также расходы на издание Трудов конференции и культурные мероприятия будут оплачены организаторами конференции. Проживание в гостинице оплачивается иностранными участниками конференции самостоятельно.

Прибытие и размещение участников

Оргкомитетом для иностранных участников будут забронированы места в гостинице и организована встреча в аэропорту.

Адрес организационного комитета

Институт информационных технологий НАНА, комн. 216
Азербайджан, Az1141, Баку, ул. Б. Вагабзаде, 9
Тел.: (+994 12) 510 31 48
Факс: (+994 12) 539 61 21
pci2012az@gmail.com
www.pci2012.science.az