УДК [378.016:004.056]:378.46

Е. В. Чернова

ПРИМЕНЕНИЕ ВИДЕОКОНТЕНТА ДЛЯ КОНТРОЛЯ ЗНАНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Чернова Елена Владимировна
HellenaChernova@mail.ru
ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», Россия, г. Магнитогорск

USING VIDEOCONTENT FOR THE CONTROL OF KNOWLEDGE IN INFORMATION SECURITY

Chernova Elena Vladimirovna
Nosov Magnitogorsk State Technical University, Russia, Magnitogorsk

Аннотация. *В статье рассказывается об аспектах применения видеоконтента для проверки знаний в области информационной безопасности и защиты информации в рамках соответствующих дисциплин. Приводятся примеры видеоконтента, применительно к конкретным проблемам информационной безопасности.*

Abstract. *The article describes the aspects of the use of video to test knowledge in the field of information security and data protection within their respective disciplines. Examples of videocontent, with reference to the specific problems of information security.*

Ключевые слова: *информационная безопасность; образование; защита информации; видеоконтент; высшее образование.*

Keywords: *information security; education; protection of information; videocontent; higher education.*

Современное мировое сообщество в последние годы всё чаще тревожат вопросы, связанные с информационной безопасностью общества, личности и государства. Многие реальные и выдуманные события нашли свое отражение в ряде художественных и документальных фильмов, сериалов, аналитических передач. Высшее образование, в свою очередь, включило в образовательные стандарты практически всех специальностей – и гуманитарных, и технических – дисциплины, посвященные основам обеспечения информационной безопасности и защиты информации. Следует заметить, что на сегодняшний день подготовка студентов в области понимания сути проблем информационной безопасности сталкивается с некоторыми трудностями – методические разработки недостаточно ярко освещают различные прикладные аспекты, да и в целом, ситуация в информационном мире меняется с поразительной скоростью. То, что было остроактуальным год назад, сегодня кажется смешным и ясным, а темы, волнующие окружающих еще не скоро будут проанализированы, систематизированы и описаны в научной и популярной литературе.

Согласно Доктрины информационной безопасности от 5 декабря 2016 года, информационная безопасность Российской Федерации – это «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечи-

ваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [1]. Мы предлагаем рассматривать понятие «информационная безопасность» как двустороннюю медаль: «с одной стороны, которая всегда на виду – информационная безопасность это обеспечение защиты и безопасности данных и информации от деятельности человека. С другой, неявной стороны, информационная безопасность – это способы и методы защиты человека от воздействия информационных потоков» [4]. Информационная безопасность страны и ее граждан – серьезная проблема для любого государства.

Однако, опыт преподавания дисциплин, связанных с вопросами информационной безопасности и защиты информации для студентов прикладных и гуманитарных специальностей, показал, что студенты чаще всего склонны принимать на веру информацию, преподносимую методической литературой и преподавателем, и не пытаться перенести ее на свой реальный опыт. Максимум успеха имеют вопросы, связанные со взломом социальных сетей, либо настройкой доступа к ним же, почте или другим аккаунтам. Вопросы антивирусной безопасности преподаются и в общеобразовательном звене, и в рамках дисциплин, связанных с сетями, либо с обучением работы с ЭВМ. Таким образом, встает вопрос – чему и как обучить студента в рамках освоения дисциплин, связанных с информационной безопасностью, а самое главное, как проконтролировать глубину понимания проблем безопасности. Как показывает практика, тестовые задания не могут позволить преподавателю проверить уровень понимания ключевых аспектов защиты информации и гуманитарных проблем информационной безопасности, а семинарские занятия не позволяют максимально погрузить студента в многоаспектность вопроса.

В современном высшем профессиональном образовании существует направление использования медиаресурсов для обучения. Медиаобразование (англ. media education) – «направление в педагогике, выступающее за изучение закономерностей массовой коммуникации (прессы, телевидения, радио, кино, видео и т.д.). Основные задачи медиаобразования: подготовить новое поколение к жизни в современных информационных условиях, к восприятию различной информации, научить человека понимать ее, осознавать последствия ее воздействия на психику, овладевать способами общения на основе невербальных форм коммуникации с помощью технических средств» [3]. «Одним из таких средств является демонстрация разнообразных видеоматериалов, художественных и научно-популярных фильмов, с их последующим анализом» [2]. По мнению Ирины Кондратенко «анализ демонстрационных материалов не позволяет формально и шаблонно выполнять задание, побуждает делать это творчески, осознанно тем самым более продуктивно» [2]. В рамках образовательного процесса по формированию общекультурных и профессиональных компетенций в области защиты информации и информационной безопасности, мы предлагаем активно использовать видеоконтент для раскрытия различных аспектов информационной безопасности, а так же для контроля знаний студентов.

В ходе изучения дисциплин, связанных с проблемами информационной безопасности и защиты информации, мы предлагаем студентам к просмотру определенный набор художественных фильмов и сериалов, наглядно демонстрирующих ту или иную проблему информационного общества. После просмотра, студенты пишут эссе о просмотренной истории, в ходе

которого отвечают на три вопроса: «Что произошло? Что породило проблему? Как этого можно было избежать?» и дают собственную оценку произошедшего события. Данное сочинение позволит преподавателю оценить уровень понимания рассматриваемой проблемы безопасности, найти узкие места и оперативно отреагировать на возможные пробелы в понимании. Некоторые, наиболее знаковые произведения имеет смысл рассматривать на семинарском занятии, посвятив время более детальному обсуждению истоков проблемы, показанных в произведении.

Рассмотрим пример. Забегая вперед, необходимо отметить, что простой пересказ данного реального эксперимента не так сильно воздействует на студентов, как просмотр фильма, снятого по сценарию автора эксперимента «Третья волна» Рона Джонсона. Фильм «Волна» («Die Welle»), 2008 года. Описание с сайта Кинопоиск «Германия. Наши дни. Школьный учитель истории предлагает своим ученикам провести эксперимент: ровно неделю старшеклассники будут жить по законам тоталитарного государства. Жесткая дисциплина, повсеместный контроль, доносы, наказания – нацистская схема воссоздается с пугающей точностью. Ученики на собственном примере убеждаются, с какой легкостью можно манипулировать людьми, превращая их в безликую покорную массу. Но в какой-то момент игра выходит из-под контроля, и теперь ее участникам предстоит дойти до конца и познать самую темную сторону диктатуры» [5]. После просмотра фильма, студенты часто остаются в недоумении – как могла сработать такая явная провокация и манипуляция? Почему школьники поддались на такую явную игру? Почему всё едва не закончилось очень плачевно? С помощью данной истории студенты могут познакомиться с такими явлениями, как информационное манипулирование и информационное зомбирование.

В качестве основных видеоматериалов можно назвать следующие: сериалы «Менталист» и «Последователи» (манипулирование, зомбирование), «В поле зрения» (глобальные проблемы информационной безопасности общества), «Черное зеркало» (фантазии на тему угроз, влекомых развитием информационных технологий), «Мистер Робот» (проблема хакерства); фильмы «Хвост виляет собакой» (манипулирование, азбука пропаганды), «Тучи над Борском» (зомбирование, манипулирование), «Не оставляющий следа» (личная безопасность в сети) и многие другие.

Помимо предлагаемого видеоконтента, необходимо побуждать студентов к поиску других произведений, тем самым, закрепляя понимание изучаемой проблемы информационной безопасности. Мы настаиваем на необходимости аналитического обоснования новых медиаматериалов, для того, чтобы студент мог подтвердить значимость своей находки.

Таким образом, применение видеоконтента для проведения контроля знаний студента в области информационной безопасности обеспечит не только качественную проверку уровня понимания материала, но и даст толчок к развитию аналитического и критического мышления.

Список литературы

1. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] – Режим доступа: http://www.scrf.gov.ru/documents/6/5.html (дата обращения: 30.01.2017)

2. Кондратенко, И.В. Особенности технологии применения видеоматериалов в учебном процессе [Текст] // Вестник Шадринского государственного педагогического университета. – 2015. – № 4 (28). – С. 31-34.

3. Медиаобразование [Текст] // Российская педагогическая энциклопедия. Т.1/Гл. ред. В.В.Давыдов. – М.: Большая российская энциклопедия, 1993. – С. 555.

4. Чернова, Е.В. Информационная безопасность для гуманитариев [Текст]: учебник для студентов вузов / Е.В. Чернова. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2016. – 280 с.

5. Эксперимент 2: Волна [Электронный ресурс] // КиноПоиск. – Режим доступа: https://www.kinopoisk.ru/film/387388/ (дата обращения: 30.01.2017)