УДК 378.147:004.056

ОБ ОПЫТЕ ПРИМЕНЕНИЯ ВИТАГЕННОГО ОБУЧЕНИЯ ПРИ ПРОВЕДЕНИИ ЗАНЯТИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАКАЛАВРОВ И МАГИСТРОВ ЭКОНОМИКИ

Овсяницкая Л.Ю.[1,2], Лысенко Ю.В.[1,3]

[1]ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Уральский филиал, Челябинск, e-mail: larovs@rambler.ru;
[2]ЧОУВО «Международный институт дизайна и сервиса», Челябинск;
[3]ФГОБУ «Южно-Уральский государственный гуманитарно-педагогический университет», Челябинск, e-mail: lysenkoyulia@mail.ru

Статья посвящена необходимости применения специализированных педагогических подходов и методов для подготовки бакалавров и магистров в области информационной безопасности в связи с быстрым ростом и качественными изменениями во всех областях жизни человека. Представлено, что в настоящее время практически вся государственная, профессиональная и персональная информация человека отображается и хранится в цифровом формате. Доказано, что компрометация или потеря этих данных информации могут привести как к репутационным, так и к финансовым потерям человека или предприятия. В работе уделено внимание возникновению нового явления в жизни людей – цифрового следа. Обосновано различие понятий пассивного и активного цифрового следа и проанализировано его влияние на безопасность человека. В работе доказано, что обучение информационной безопасности не сводится к традиционному изучению технических и организационных аспектов вопроса. Подробно показана необходимость привлечения витагенного опыта студентов при преподавании информационной безопасности в высших учебных заведениях, поскольку именно витагенный подход способствует осознанию необходимости соблюдения правил информационной безопасности. В работе описаны применяемые авторами педагогические подходы и методы. Представлены конкретные примеры и задания для проведения практических занятий со студентами с использованием витагенного обучения. Результатом является осознание обучающимися необходимости соблюдения правил и норм информационной безопасности.

Ключевые слова: информационная безопасность, витагенное обучение, высшая школа.

ABOUT THE EXPERIENCE OF APPLICATION OF VITAGENIC LEARNING IN CONDUCTING CLASSES ON INFORMATION SECURITY OF BACHELORS AND MASTERS OF ECONOMY

Ovsyanitskaya L.Y.[1,2], Lysenko Y.V.[1,3]

[1]Financial University under the Government of the Russian Federation, Ural branch, Chelyabinsk, e-mail: larovs@rambler.ru;
[2]International Institute of Design and Service, Chelyabinsk;
[3]South Ural State Humanitarian Pedagogical University, Chelyabinsk; e-mail: lysenkoyulia@mail.ru

The article is devoted to the need to apply specialized pedagogical approaches and methods for training bachelor's and master's degrees in the field of information security in connection with the rapid growth and qualitative changes in all areas. It is presented that at present, almost all state, professional and personal information of a person is displayed and stored in digital format. It has been proven that the compromise or loss of this information can lead to both reputational and financial losses to a person or company. The work focuses on the emergence of a new phenomenon in people's lives - a digital footprint. The difference between the concepts of passive and active digital footprint is substantiated and its impact on human safety is analyzed. The paper proves that information security training is not limited to the traditional study of technical and organizational aspects of the issue. The process of the need to attract the vitagenic experience of students when teaching information security in higher educational institutions is shown in detail, since it is the vitagenic approach that promotes awareness of the need to comply with information security rules. The paper presents the pedagogical approaches and methods used by the authors. Specific examples and tasks for conducting practical exercises with students using vitagenic learning are presented. The result is students' awareness of the need to comply with the rules and regulations of information security.

Keywords: information security, vitagenic learning, high school.

В настоящее время вся бытовая, общественная и профессиональная деятельность людей подвержена цифровой трансформации. Согласно статистическим данным, количество пользователей портала Госуслуги составляет приблизительно 75% жителей России и продолжает постоянно увеличиваться [1]. Более 2/3 населения страны доверили все свои персональные данные электронной системе. Другие порталы: банковские системы, многочисленные личные кабинеты в интернет-магазинах, учебных, развлекательных сайтах и иные – суммарно могут иметь даже больший охват.

Как известно, для обеспечения безопасности и конфиденциальности применяются программные и аппаратные комплексы, в основе которых лежат математические алгоритмы, которые имеют высочайшую степень устойчивости ко взлому. Но ни один алгоритм не устоит против человеческого фактора, который выражается в безграмотных действиях или, напротив, бездействии при осуществлении процедуры входа и работе с электронными ресурсами, использовании стандартных однотипных паролей, отказе от установки антивирусного программного обеспечения, несоблюдении организационно-правовых норм при работе с ключами электронной подписи. Компрометация персональных данных в настоящее время может грозить не только временными и репутационными, но и финансовыми потерями.

Следующий фактор, который был не очень важным еще несколько лет назад, но приобретает особую значимость сейчас, – это цифровой след. Этот термин имеет синонимы: «цифровой отпечаток», «цифровая тень», «кибертень». Цифровым следом является информация о пользователе, которая остается в Интернете после просмотра сайтов [2]. След будет пассивным, если пользователь только просматривает страницы, и активным, если он оставляет комментарии, ведет переписку, оставляет «лайки». В совокупности анализ интернет-активности человека создает его виртуальный образ, который активно используется интернет-маркетологами. Появился термин «доксинг» (поиск открытой и конфиденциальной информации о человеке без его ведома).

С одной стороны, получение таргетированной рекламы в разумных количествах полезно пользователям и коммерческим организациям, ведет к повышению качества обслуживания клиентов, с другой стороны, ситуация гораздо глубже и серьезнее.

Виртуальный образ пользователя можно представить своеобразной системой фильтров, которые отслеживают, анализируют и ранжируют по степени значимости для пользователя товары, места, друзей. Постепенно вокруг человека создается информационный «микроклимат». В его персональное виртуальное пространство в социальных сетях с большой долей вероятности попадут рекомендуемые ему товары и услуги, друзья, разделяющие его мнение и интересы. Большое количество подобных друзей

постепенно могут воздействовать на мировоззрение и мотивы человека, способствуя приобретению товаров или услуг [3].

Работодатели все чаще признают, что информация, доступная на сайтах социальных сетей, влияет на кадровые решения, включая набор, обучение, продвижение по службе и увольнение [4]. Более того, 70% опрошенных менеджеров по подбору персонала отклоняли кандидатов на работу из-за их ненадежной репутации в Интернете.

Вопросам информационной безопасности, на наш взгляд, уделяется очень мало внимания в процессе среднего, высшего и дополнительного профессионального обучения. Технология и педагогические подходы к преподаванию чаще всего стандартные: лекционные и практические задания, ознакомление с теоретическими аспектами вопроса, решение задач.

Однако такие традиционные методы абсолютно не подходят к осознанию жизненной важности вопроса. Прослушав лекцию и решив задачу, студент, возможно, будет знать о существующих нормативных актах, организационно-правовых нормах и технических мероприятиях, но он не будет осознавать неукоснительность их выполнения, поскольку не понимает, что риски, о которых говорит преподаватель, не виртуальны, а непосредственно касаются его лично, его друзей и родственников. Он не будет тратить личное время и деньги на обеспечение информационной безопасности.

Поэтому нами была разработана технология обучения студентов информационной безопасности на основе их витагенного опыта. Любой студент обладает бытовым, социальным или профессиональным жизненным опытом, который должен быть использован как полезный и важный источник обучения.

А.С. Белкин предложил витагенный подход к обучению [5]. Этот подход основывается на актуализации или востребовании жизненного опыта человека, его интеллектуального, психологического, нравственного потенциала.

А.С. Белкин разделил опыт жизни и жизненный (витагенный) опыт. Под опытом жизни можно понимать всю информацию, полученную человеком в течение его осознанной жизни. Под жизненным (или витагенным) опытом можно представлять информацию, которая уже является достоянием личности, сохранена в долговременной памяти, находится в состоянии готовности к применению. Она важна и актуальна для человека.

При этом переход опыта жизни в жизненный (или витагенный) опыт осуществляется только тогда, когда оказалось, что жизненный опыт имеет социальную или ценностную значимость, он необходим для решения возникшей проблемы или позволяет прогнозировать и конструировать будущее, анализируя собственные ошибки или достижения.

Анализируя собственный педагогический опыт и опыт наших коллег [6, 7], мы понимаем, что именно витагенный подход в преподавании информационной безопасности

студентам высшего образования позволит разработать технологию обучения, кардинально отличающуюся от приведенной выше.

Целью исследования является разработка технологии проведения занятий таким образом, чтобы все изучаемые темы:

– рассматривались и обсуждались с точки зрения личной безопасности студента, его родственников или друзей;

– могли подтвердить социальную значимость конкретного вопроса и масштаб поднятой проблемы не декларативно, а с основой на результатах научного эксперимента, который был инициирован и проведен студентом;

– основывались на ситуациях, которые происходили в реальной жизни студентов, их друзей или родственников;

– требовали привлечения жизненного (витагенного) опыта решения данной проблемы. При этом витагенный опыт студента может быть не только успешным, но и отрицательным.

Представим адаптацию идей А.С. Белкина и Н.О. Вербицкой для создания методологии формирования компетентности студентов в области информационной безопасности [8].

Для решения поставленной задачи нами был проведен анализ педагогических подходов, методов и принципов, на основе которых будет разрабатываться технология обучения. Нами были выбраны следующие подходы и методы.

Голографический (многомерный) подход

Как известно, голографическое изображение – это изображение, позволяющее человеку наблюдать объект под разными углами, с разных сторон. Принцип физического явления лег в основу голографического или, его еще называют, многомерного подхода в образовании.

В работе [9] автор утверждает, что для того, чтобы человек овладел пониманием, а не имел перечень знаний, ему необходим голографический портрет явления, а это возможно только при наличии различных интерпретаций вопроса. Голографический (или многомерный) подход предполагает применение различных технологий, методов, приемов, форм и средств, которые позволяют представить изучаемый объект во всех его измерениях и проявлениях, под разным углом зрения.

Пример применения голографического подхода.

1. Тема занятия: «Спам».

Спамом называют массовую рассылку корреспонденции рекламного характера, преимущественно электронных писем или сообщений, людям, которые не выразили желания ее получать. Чаще всего спам содержит рекламу товаров или услуг.

На спам некоторые люди не обращают внимания, другим он кажется раздражающим фактором, действием, несущим опасность путем возможных вредоносных включений, явлением, отнимающим дорогое рабочее время сотрудников, работой мошенников. Однако присутствуют и те, кому рассылка спама приносит деньги: рекламодатели, рекламные агентства, поставщики и отправители спама. Некоторые получатели находят в спаме полезную для себя информацию, поскольку спам становится таргетированным. Достаточно сложна и юридическая интерпретация данного явления.

Такой разный взгляд на одно явление требует его рассмотрения с точки зрения всех участников процесса – от заказчиков спама до исполнителей и получателей. При проведении занятия применяется голографический подход, позволяющий оценить одно явление с различных позиций и выработать собственное суждение. В ходе деловой игры студенты представляют себя в разных ролях, изучают это неоднозначное явление с разных сторон.

Итогом занятия является понимание того, что:

– за каждым случаем появления вредоносной программы или спама стоит материально заинтересованное лицо, финансирующее данный проект. Создание вирусов и рассылка спама – это не раздражающий фактор, а хорошо организованный бизнес;

– имеется необходимость установки современного лицензионного программного обеспечения для защиты от вредоносных программ.

– необходимы умения и навыки выполнения элементарных действий, препятствующих заражению компьютера вирусами.

2. Тема занятия: «Защита информации путем ее преобразования. Основные направления использования криптографических методов».

На занятиях мы имитируем процесс электронного документооборота: студенты создают электронные ключи шифрования, обмениваются самостоятельно зашифрованными и/или подписанными электронными сообщениями, отрабатывают шаблоны поведения добросовестных участников документооборота, имитируют действия злоумышленников, пытающихся подменить текст или авторство документа и использующих методы социального инжиниринга для доступа к паролям, узнают о характерных приемах социального инжиниринга.

Ознакомление с психологическими аспектами и основными шаблонами социального инжиниринга – способов и приемов обмана людей, приводящих к тому, что они сами предоставляют пароли или иную информацию, которая помогает злоумышленникам

нарушить безопасность системы, а также рассмотрение объектов изучения с различных, противоположных сторон позволяют:

– осознать практически абсолютную надежность алгоритмов и процедур электронного документооборота по защите передаваемой информации, но одновременно и возможность компрометации информации при нарушении пользователями элементарных правил;

– сформировать грамотное отношение к генерации, использованию, хранению и уничтожению ключей электронной подписи, исключающее вмешательство человеческого фактора в алгоритмы защиты информации.

Эвристическое обучение (от греч. Heurisko – «отыскиваю, нахожу, открываю»)

Целью эвристического обучения являются поиск и осознание студентом собственного смысла, целей и содержания явлений и процессов, постоянное открытие новых, часто неожиданных, аспектов и сторон изучаемого предмета.

Пример применения эвристического обучения

Тема занятия: «Правила выбора паролей. Расчет энтропии и битового пространства паролей». На занятии мы сначала рассчитываем энтропию и битовое пространство паролей и обосновываем на основе полученных данных необходимое количество и варианты символов для различных информационных систем, проводим мозговой штурм, позволяющий создать собственные мнемонические правила для возможности запоминания криптографически стойкого к попыткам взлома пароля.

Результат:

– сформированный навык распознавания атаки злоумышленников, направленной на пользователей информационной системы с целью овладения информацией о паролях;

– умение рассчитывать необходимое количество и варианты используемых символов создаваемого пароля в зависимости от назначения информационной системы.

Принцип интерактивности (от англ. Interaction – «взаимодействие») и фасилитации (от англ. Facilitate – «облегчать, способствовать, создавать благоприятные условия»).

Эти принципы основываются на взаимодействии участников учебного процесса: педагога и студентов, студентов между собой – путем использования современных средств коммуникации. При фасилитации обучения педагог занимает позицию не «над», а «вместе» с обучаемыми, он формирует умение делать выводы, находить новые грани проблем в рассматриваемой ситуации.

Целью использования данного принципа является создание комфортных условий обучения, которые способствуют тому, чтобы обучающиеся могли почувствовать свою успешность и интеллектуальную состоятельность. Процесс обучения предполагает

дискуссии и диалоги, ведущие к совместному решению значимых лично для каждого студента задач.

Аутентичное оценивание – оценивание сформированности умений и навыков студентов по защите информации путем помещения их в ситуацию, максимально приближенную к реальной повседневной или профессиональной жизни.

Тема занятия: «Идентификация, аутентификация, авторизация пользователей. Особенности обработки, хранения и передачи персональных данных».

После изучения теоретического материала студенты имитируют роли оператора и владельца персональных данных. Отрабатываются сценарии действий в случае личного и дистанционного общения участников, использования известных информационных систем с хранением информации о персональных данных в «облаке», находящемся в России и за рубежом. Анализируются существующие угрозы у собственного смартфона или домашнего компьютера, вырабатываются меры для минимизации рисков.

Результат: осознание возможности реального ущерба при несоблюдении простейших правил информационной безопасности; приобретение умений и навыков минимизации рисков на смартфоне и домашнем компьютере; понимание того, что и домашний компьютер содержит информацию, дискредитация которой может привести к финансовым и временным потерям.

Студенты, которых заинтересовала данная тема, продолжают изучать ее более углубленно. Тема становится основой будущей статьи на конференцию.

Выводы

Применение витагенного обучения по итогам анализа многолетнего опыта авторов преподавания информационной безопасности в вузах позволило рассмотреть все изучаемые темы и задачи с точки зрения личной безопасности студента, опираясь не только на теоретические знания, а в большей степени на витагенный опыт обучающихся. Результатом является глубокое понимание и осознание того, что малейшее несоблюдение простейших правил информационной безопасности может привести к реальному финансовому или репутационному ущербу.

Авторы статьи – победители грантового конкурса Стипендиальной программы Владимира Потанина 2018/2019 / Издано с использованием гранта Благотворительного фонда Владимира Потанина, № ГК190001792.

Список литературы

1. Аудитория и статистика портала Госуслуг. [Электронный ресурс]. URL: http://zdrav.expert/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%90%D1%83%D0%B4%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D1%8F_%D0%B8_%D1%81%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0_%D0%BF%D0%BE%D1%80%D1%82%D0%B0%D0%BB%D0%B0_%D0%B3%D0%BE%D1%81%D1%83%D1%81%D0%BB%D1%83%D0%B3 (дата обращения: 20.10.2020).
2. Шамсутдинова Т.М. Когнитивная модель траектории электронного обучения на основе цифрового следа // Открытое образование. 2020. Т. 24. № 2. С. 47-54.
3. Sjöberg M., Chen H., Floréen P., Koskela M., Kuikkaniemi K., Lehtiniemi T., Peltonen J. Digital me: Controlling and making sense of my digital footprint. 5th International Workshop on Symbiotic Interaction. Springer. Cham. 2016. P. 155-167.
4. Brown V.R., Vaughn E.D. The use of social networking in hiring decisions. Journal of Business & Psychology. 2011. no 26. P. 219-255. DOI: 10.1007/s10869-0111-9221-x.
5. Белкин А.С., Вербицкая Н.О. Витагенное образование в системе педагогического знания (витагенная концепция личности) // Педагогическое образование в России. 2007. № 1. С. 26-32.
6. Овсяницкая Л.Ю. Теоретико-методологические основы формирования информационной компетентности специалистов системы здравоохранения: монография. М.: Издательство «Перо», 2015. 163 с.
7. Cox C., Gunderman R. Andragogic Approaches to Continuing Medical Education. Educational perspective. 2017. vol. 24. no 10. P. 1325-1326. DOI: 10.1016/j.acra.2017.05.004.
8. Белкин А.С. Основы возрастной педагогики: учеб. пособие для студ. высш. пед. учеб. заведений. М.: Издательский центр «Академия», 2000.192 с.
9. Татаренкова И.А., Кибец В.Н. Преподаватель как фасилитатор инновационного образовательного процесса в вузе // Современные проблемы науки и образования. 2015. № 1-1. [Электронный ресурс]. URL: http://science-education.ru/ru/article/view?id=18086 (дата обращения: 07.10.2020).