УДК 007.3

НОВЫЙ ПОДХОД К ПРЕПОДАВАНИЮ ВВОДНОГО КУРСА КИБЕРБЕЗОПАСНОСТИ

Тулупова И.С.

Студент 2 курса,

ФГБОУ ВО "Поволжский Государственный Университет Телекоммуникаций и Информатики"

Самара, Россия

Аннотация. В современном мире технологии повсеместны. Сегодняшние дети растут с большим количеством технологий, таких как телефоны, игровые системы, планшеты и компьютеры. Даже «вещи» подключены к Интернету. К таким вещам относятся дверные замки, кофеварки, холодильники, термостаты и динамики, и это лишь некоторые из них. Устройств Интернета вещей больше, чем людей во всем мире. Связанные вещи изменили жизни людей и мира во многих положительных аспектах, но они также связаны с многочисленными проблемами безопасности и конфиденциальности. Таким образом, образование в области кибербезопасности стало решающим в обеспечении осведомленности о безопасности, безопасного поведения и опыта в области кибербезопасности. В этой статье обсуждается новый подход к обучению кибербезопасности, и оценивается эффективность предложенного подхода.

Ключевые слова: кибербезопасность, обучение, обучение кибербезопасности, письмо, проекты, прозрачное задание

A NEW APPROACH TO TEACHING AN INTRODUCTARY CYBERSECURITY COURSE

Tulupova I.S.

Student 2 course

Volga state University of telecommunications and Informatics,

Samara, Russia

Abstract. In the modern world, technology is ubiquitous. Today's children are growing up with a lot of technology, such as phones, gaming systems, tablets, and computers. Even "things" are connected to the Internet. These things include door locks, coffee makers, refrigerators, thermostats, and speakers, to name just a few. There are more IOT devices than there are people around the world. Connected things have changed people's lives and the world in many positive ways, but they also involve numerous security and privacy issues. Thus, education in the field of cyber security has become crucial in ensuring awareness about safety, safe behavior and experience in the field of cybersecurity. This article discusses a new approach to cybersecurity training and assesses the effectiveness of the proposed approach.

Keywords: cybersecurity, training, cybersecurity training-writing, projects, transparent task

1 Введение

Мы живем в эпоху, когда количество персональных компьютеров превышает численность всего населения. В 2016 году в 85% домохозяйств США был хотя бы один смартфон, настольный или портативный компьютер, планшет или потоковое устройство. В «типичном» домохозяйстве было пять таких устройств [1]. Внедрение технологий, подключенных к Интернету, находится на подъеме. Gartner прогнозирует, что к 2021 году во всем мире будет более 20 миллиардов устройств Интернета вещей (IoT) [2-3]. В это число не входят компьютеры и телефоны. За последние пять лет было взломано около 15 миллиардов записей, содержащих личную информацию, что затронуло почти все секторы промышленности, включая социальные сети, гостиничный бизнес, технологии, розничную торговлю, развлечения, некоммерческие организации, правительство, здравоохранение, образование и финансы [4]. Нарушения данных имеют большое финансовое и психологическое воздействие на людей, а предприятия несут огромные финансовые потери, иногда приводящие к банкротству. В дополнение к атакам, затрагивающим отдельных лиц, таким как кража личных данных, уже имели место крупномасштабные атаки, такие как распределенный отказ в обслуживании Mirai (DD0S). Mirai обрушился на

крупные предприятия, затронув миллионы пользователей [5]. В связи с быстрым распространением подключенных технологий мы можем только ожидать роста инцидентов в области кибербезопасности.

Таким образом, существует растущая потребность в осведомленности о кибербезопасности для всех и образовании в области кибербезопасности на всех академических уровнях. Это привело к увеличению количества программ кибербезопасности в образовательных учреждениях, сертификации кибербезопасности в отрасли и спросу на рабочие места среди персонала. В этой статье я обсуждаю новый педагогический подход TWOPD, используемый для преподавания учебной программы по кибербезопасности в курсе ITN 260 (называемый в этой статье «пилотным курсом»), и представляю результаты его оценки. Оценка показывает, что подход эффективен с точки зрения уровня удовлетворенности студентов. Вклады этого документа заключаются в следующем: (а) он представляет TWOPD, новый подход к преподаванию курса кибербезопасности, и (б) в нем обсуждаются результаты оценки подхода.

2 Связанные работы

Winkelmes (2013) изучал прозрачность обучения и преподавания и опубликовал прозрачный шаблон задания, который содержит компоненты: цель, задачи и критерии успеха [6]. После этого важность прозрачных заданий широко изучалась, и многие преподаватели приняли ее. Прозрачный дизайн демонстрирует актуальность задания для обучения студентов, разъясняет действия и позволяет студентам самостоятельно оценивать задание [7]. Письмо помогает учащимся осмыслять сложные идеи, выражать их и лучше учиться. Стратегии письма для обучения изучаются в научных и других дисциплинах. Gunel et al. (2007) провели вторичный анализ шести исследований, посвященных письму в науке, и обнаружили, что студентам больше пользы от письма для обучения, чем от научного письма, и что они набрали больше баллов [8]. Онлайн-курсы, если они хорошо разработаны, могут предложить учащимся множество

педагогических преимуществ, помимо гибкости во времени и географических границах. Рост числа онлайн-курсов, массовых открытых онлайн-курсов (MOOCS) и онлайн-степеней - свидетельство этого аргумента. Glance et al. (2003) показали, что онлайн-курсы могут быть лучше и эффективнее очных.

Прошлые исследования продемонстрировали преимущества проектного обучения (PBL). Исследователи показали, что PBL помогает студентам получить более глубокое понимание концепций, когда они заняты решением проблем. Студенты также успевают лучше, чем в традиционных форматах [9]. Демонстрации - важный метод обучения людей [10] и роботов. У студентов есть разные стили обучения, а демонстрации дают студентам возможность визуализировать продемонстрированные концепции и формулировать идеи. Демонстрации помогают студентам формировать аргументы, ставить под сомнение существующие концепции и генерировать новые исследовательские идеи [10].

3 Подход

Подход основан на лучших педагогических подходах к онлайн и очным курсам. Подход ПНОПД (TWOPD) состоит из следующих элементов:

1. Прозрачные задания (**T**ransparent assignment)

2. Написание (**W**riting)

3. Онлайн-дизайн (**O**nline Design)

4. Проекты (**P**rojects)

5. Демонстрации (**D**emonstrations)

3.1 Прозрачные задания

Прозрачное задание состоит из трех основных компонентов: цели, задач и критериев успеха. Цель задания показывает четкую связь задания с обучением

студентов, результатами обучения и актуальностью задания для функций кибербезопасности в реальном мире. Когда студенты видят связь задания с их собственным обучением, у них появляется мотивация выполнить его с большим интересом. Компонент «задачи» перечисляет действия, которые выполняет студент. В компоненте «Критерии успеха» перечислены характеристики завершенного задания и критерии оценки.

3.2 Письмо

Письмо укрепляет обучение. Письмо позволяет учащимся выражать изученные концепции, чтобы другие читали и учились. Однако в области информационных технологий (ИТ) глобальные отраслевые сертификационные экзамены основываются на вопросах с несколькими вариантами ответов, а также на вопросах, основанных на сценариях или результатах, которые имеют преимущество автоматической оценки и мгновенного уведомления о результатах. Следовательно, введение письма часто наталкивается на сопротивление и критикуется как дополнительное бремя. Письмо дает множество преимуществ, например, помогает студентам изучать концепции невидимых технологий и ясно выражать эти концепции, что часто упускается из виду на занятиях по ИТ. Учащиеся, которые хорошо пишут, имеют потенциал для успешной работы не только на уроках письма, но и в других классах, и, вероятно, продвинутся дальше в своем образовательном стремлении. На рабочем месте хорошие письменные навыки дают им возможность объяснять концепции ИТ своим коллегам, ИТ-специалистам и людям, не имеющим технического образования. Письмо в сочетании с коммуникативными навыками и навыками презентации является востребованным навыком в отрасли. Работодатели в нашем регионе назвали хорошие коммуникативные навыки основным требованием для работы в сфере информационных технологий и кибербезопасности. Технические специалисты, такие как инженеры по кибербезопасности, нуждаются в этих навыках для продвижения на

управленческие и руководящие должности. Таким образом, практика письма на наших курсах готовит наших студентов к процветанию и развитию в отрасли на всех уровнях работы. Включение письма в курс не только помогает развивает письменные навыки у студентов, но также позволяет передавать полученные навыки от академических кругов рабочей силе. Чтобы воспользоваться преимуществами письма при обучении, пилотный курс включал письменные упражнения. На каждом собрании класса ученики получали письменные упражнения, которые содержали вопросы о содержании кибербезопасности предыдущего собрания класса. Половина письменных упражнений была импровизирована. Другая половина была предварительно опубликована в системе управления обучением. Студенты должны были изучить содержание последнего урока при подготовке к упражнению. Письма студентов по вопросам упражнений мгновенно получили отклики от сверстников и инструктора. Эти письменные упражнения были разработаны, чтобы помочь студентам убедиться, что они поняли сложные концепции кибербезопасности и могут выразить или поделиться ими своими словами. Я считаю, что это подготовит их не только к выполнению функций кибербезопасности на работе, но и к тому, чтобы делиться и вносить свой вклад в команду.

3.3 Онлайн-дизайн

Курс был разработан таким же самостоятельным и независимым, как онлайн-курс. Он был разработан с использованием Blackboard, онлайн-СУО. Курс начался с ориентации на онлайн-обучение, что дало студентам возможность ознакомиться с навигацией по курсу. Содержание курса было разделено на модули по неделям. Каждый еженедельный модуль содержал следующие элементы:

• Краткое изложение учебных заданий;

• Чтение на неделю;

• Слайды преподавателя;

• Ссылки на онлайн-материалы и видео, относящиеся к содержанию недели;

• Практические викторины;

• Задания с инструкциями и сроками выполнения;

• Практические проекты;

• Экзамены и другие оценки;

• Как подготовиться к личной встрече;

• Подготовка к следующей неделе;

Курс также был дополнен такими ресурсами, как книги, видео, учебные пособия и практические экзамены.

3.4 Проекты

Этот курс был не только сосредоточен на изучении концепций путем обсуждения. Проекты имели около трети веса в учебных материалах и оценках. В курс были включены три типа проектов:

1. Краткие наборы проектов

2. Практические проекты

3. Долгосрочные проекты в конце семестра.

3.5 Демонстрации

Демонстрации оказались полезными для помощи учащимся в визуализации концепций кибербезопасности. Они помогли развить практические навыки, коммуникативные навыки и командные навыки, которые являются ключевыми для любой работы в сфере кибербезопасности. Демонстрации в классе проводились как преподавателями, так и студентами.

3.5.1 Демонстрации инструкторов

Каждое собрание в классе включало 5-10 демонстраций концепций кибербезопасности. Демонстрации были построены на очных встречах в классе таким образом, чтобы они давали возможность отдохнуть от лекции и пробудили интерес к обсуждаемым темам.

3.5.2 Демонстрации учеников

Каждый ученик должен был продемонстрировать в классе одну концепцию кибербезопасности. Студентам было разрешено выбрать тему для демонстрации по своему выбору, а инструктор следил за демонстрациями для оценки.

3.6 Дополнительная поддержка

В дополнение к пяти элементам подхода TWOPD, обучение было дополнено следующей дополнительной поддержкой студентов в курсе: а) личные групповые встречи, которые включали лекции, обзор сложных концепций, обсуждения сценариев, циклический перебор вопросы-ответы, викторины и практические упражнения, б) обязательные индивидуальные встречи, которые включали разъяснение сложных концепций кибербезопасности, объяснение запрошенного студентами материала и помощь в выполнении практических упражнений и проектов. Эти занятия координировались и проводились инструктором по просьбе студентов.

4 Обсуждение и выводы

В подходе ПНОПД (TWOPD) использовались лучшие методы личного и онлайн-обучения. Прозрачный дизайн заданий позволил прояснить ожидания преподавателя и ученика, сведя к минимуму непонимание инструкций. Первоначально студенты возражали против написания курса по кибербезопасности, ссылаясь на сертификационные экзамены, не содержащие письменных вопросов. Однако после нескольких модулей отказ исчез, и

студенты начали ценить письменную помощь, оказываемую им в обучении. Онлайн-дизайн курса позволил студентам получить доступ к полному, самостоятельному курсу с учебными материалами и заданиями, которые всегда у них под рукой. Проекты научили студентов выполнять задачи по кибербезопасности. Демонстрации позволили им научиться делиться своей работой и общаться в командах. Подход ПНОПД (TWOPD) оказался эффективным для достижения высокого уровня удовлетворенности студентов пилотным курсом и повышения качества обучения студентов. Одним из ограничений исследования является небольшой размер выборки. Исследование можно расширить, включив в него больше результатов опроса. Еще одно ограничение - в педагогическом подходе. Было бы желательно оценивать все практические проекты, если позволяют ресурсы, такие как время и наличие помощников преподавателя. Однако для исследования оценивались только наборы проектов путем тщательного отбора тех, которые соответствуют результатам обучения по курсу. В будущем следует изучить возможность использования этого подхода в других курсах по кибербезопасности и его более масштабную оценку. Также будет полезно изучить, может ли подход ПНОПД (TWOPD) работать эффективно при преподавании практических курсов по кибербезопасности, таких как тестирование на проникновение, когда студентам требуется много времени для самостоятельного изучения инструментов.

Библиографический список

1.Треть американцев живет в семье с тремя и более смартфонами [Электронный ресурс] // Display PPT file. URL: https://pewrsr.ch/2r0o06he (дата обращения 19.07.20)

2. Бобков, Е.О. Обеспечение информационной безопасности критической информационной инфраструктуры с IOT-технологиями. / Е.О. Бобков, Е.А. Балашова, Д.Н. Панин. // Экономика и общество: перспективы развития. Сборник материалов IV Всероссийской научно-практической конференции. - Киров, 2020. -С. 221-225.

3. Бобков, Е.О. Анализ кибератак на критическую информационную инфраструктуру с IOT-технологиями / Е.О. Бобков, Е.А. Балашова, Д.Н. Панин // Автономия личности. 2020. № 2 (22). С. 55-64.

4. Hung, M. Leading the IoT. Gartner / M. Hung // Informatization and communication. - 2017

5.Индекс уровня нарушений [Электронный ресурс] // Display PPT file. URL: https://breachlevelindex.com/. (дата обращения 19.07.20)

6. April, T., Zhou, Y. Understanding the Mirai Botnet. In:, Proceedings of the 26th USENIX Security Symposium / April, T., Bailey, M., Burstein, E., Cochran, J., Durumeric, Z., Alex Halderman, J., Mensher, D., Seaman, K., Sullivan, N., Thomas, K., Zhou, Y. // Understanding the Mirai Botnet. In:. – Vancouver , 2017.

7. Панин, Д.Н Облачная безопасность-рекомендации по снижению угроз / Д.Н Панин, Д.Н. Филиппова, Д.С. Пирогов// Информатизация и связь. 2020. № 2. С. 73-76.

8. Обучающая интервенция, что увеличивает успеваемость студентов колледжей с недостаточным уровнем обеспеченности услугами смартфонами [Электронный ресурс]// Display PPT file. URL:https://tilthighered.com/assets/pdffiles/Transparent%20Assignment%20Template.pdf (дата обращения 10.08.20)

9. Gunel, M. Письмо для обучения в науке: вторичный анализ шести исследований [Электронный ресурс] // Display PPT file. URL: https://doi.org/10.1007/s10763-007-9082-y (дата обращения 10.08.2020)

10. Kirk, J. Интерактивное изучение целей задач с наглядными демонстрациями. / J. Kirk, A. Meininger, J. Laird //Biol. Inspired Cogn. Archit. – 2016

Оригинальность 97%