УДК 378:004.056

А. Е. Водясов

Д. М. Кирюхин

В. Г. Сидоренко, докт. техн. наук

ООО «СЕК-КОНСАЛТ СЕРВИСЕЗ»

Кафедра управления и защиты информации,

Российский университет транспорта, Москва

ОПЫТ ПОДГОТОВКИ КАДРОВ ДЛЯ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ТРАНСПОРТНОЙ ОТРАСЛИ

В условиях пандемии роль специалистов в области компьютерной безопасности при решении задач бесперебойной работы транспортных предприятий возросла многократно. Статья посвящена подведению итогов и анализу опыта, накопленного в РУТ (МИИТ) за 20 лет подготовки специалистов по специальности «Компьютерная безопасность», определению перспектив развития образовательной программы. Представлена методика использования свободно распространяемого программного обеспечения, созданного авторами статьи, в процессе обучения, когда оно невозможно или небезопасно на реальных объектах. Основное преимущество методики в том, что она учитывает опыт, полученный специалистами при решении реальных кейсов, позволяет воспроизводить без вреда для реальных систем в учебных целях уязвимости систем, дает возможность диагностировать эти уязвимости, эксплуатировать их, выбирать и сравнивать различные пути их удаления из системы. Статья содержит анализ публикаций, посвященных опыту подготовки кадров по специальности «Компьютерная безопасность» в разных странах с использованием различных инструментов. Дан обзор образовательной программы и сформулированы принципы, положенные в основу подготовки в Российском университете транспорта. Продемонстрированы примеры применения цифровых двойников в процессе обучения, сделан акцент на формировании междисциплинарных связей, навыков применения теоретических знаний для решения практических задач и анализа полученных результатов. Выполнен обзор тем дисциплины «Методы анализа управления рисками», статистический анализ результатов практической реализации разработанной авторами методики, их графическая интерпретация. Показаны варианты применения теории рисков к решению задач компьютерной безопасности. Статья содержит примеры участия обучающихся в исследовательской деятельности, создании методического обеспечения соответствующей образовательной программы, различных мероприятиях вне стен университета.

Компьютерная безопасность, подготовка кадров, цифровой двойник, уязвимость, риск

DOI: 10.20295/2412-9186-2021-7-2-315-335

Введение

В настоящее время в соответствии со Стратегией развития информационного общества в Российской Федерации на 2017–2030 годы и программой «Цифровая экономика Российской Федерации» в государственных компаниях, в т. ч. ОАО «РЖД», активно внедряются новые информационные технологии, что повышает актуальность решения задач компьютерной безопасности (КБ).

Разработанные Минкомсвязи России методические рекомендации по переходу на отечественное программное обеспечение сейчас апробируются в ОАО «РЖД» и других ведущих госкомпаниях страны. Холдинг в тесном сотрудничестве с разработчиками тестирует созданные в рамках реализации стратегии импортозамещения программные продукты и платформы для ведения электронного документооборота, управления данными и т. д. Разработчики отечественного программного обеспечения должны при внедрении учитывать возможные риски, связанные с непрерывностью технологического цикла на сети, а также количество пользователей — сотрудников компании, партнеров и контрагентов «РЖД» [1]. В соответствии с концепцией «Цифровая железная дорога» в рамках создания Комплексной системы обеспечения безопасности населения на транспорте в условиях пандемии холдинг обеспечил бесперебойную удаленную работу тысячам сотрудников компании с помощью специальных средств защиты информации от несанкционированного доступа. Специалисты в области компьютерной безопасности, получившие соответствующее образование в стенах Российского университета транспорта, принимают активное участие в этой работе [2].

Обучение студентов по специальности «Компьютерная безопасность» началось в университете в 2001 году. Приближающееся 20-летие с начала подготовки по специальности требует подведения итогов и определения перспектив развития образовательной программы (ОП).

Целью статьи является представление уникальной методики использования для подготовки специалистов по компьютерной безопасности свободно распространяемого программного обеспечения (ПО), созданного авторами статьи, в случаях, когда это невозможно делать на реальных объектах. ПО позволяет симулировать уязвимости компьютерных систем и их реакцию на воздействие различных инструментов. Применение этого ПО в учебном процессе позволяет формировать навыки и умения тестирования безопасности компьютерных систем и повышения их защищенности. Основное преимущество методики в том, что она учитывает опыт, полученный специалистами при решении реальных кейсов, позволяет воспроизводить без вреда для реальных систем в учебных целях уязвимости систем, дает возможность диагностировать эти уязвимости, эксплуатировать их и выбирать пути их удаления из системы. В случае неудачи у учащихся всегда есть шанс испробовать другой путь и достичь цели. Многие задачи имеют несколько путей решения, что позволяет сравнить их и выбрать рациональный вариант. Делать это в реальных системах небезопасно.

Уникальность методики и ее отличие состоит в использовании постоянно обновляемого ПО, которое учитывает новейшую информацию об уязвимостях компьютерных систем и опыт разработчиков в их преодолении. Это программное обеспечение можно рассматривать в качестве тренажера для специалиста по КБ. Широкий спектр задач разного уровня сложности и направленности и необходимость подготовки развернутого отчета по результатам выполнения

заданий позволяют закрепить теоретические знания и выстроить логические связи. Это определяет положительный эффект от внедрения методики.

Множество работ посвящено анализу опыта подготовки специалистов по КБ на разных уровнях образования [3] — как в нашей стране [4], так и за рубежом [5–10]. В работах [11–16] рассматриваются методики организации обучения, в т. ч. на производстве [17]. Во многих из них показаны аспекты применения цифровых двойников для решения задач и эффективность такого подхода [18–21].

Принципы организации подготовки кадров для обеспечения КБ транспортной отрасли

В связи с изменением федеральных государственных образовательных стандартов и учетом накопленного опыта подготовки специалистов и требований работодателей учебный план по специальности неоднократно менялся. В настоящее время подготовка ведется в соответствии со стандартом высшего образования РУТ (МИИТ) (самостоятельно утверждаемым образовательным стандартом) по специальности 10.05.01 — «Компьютерная безопасность».

В основу создания ОП заложены принципы, направленные на формирование у учащихся следующих компетенций, знаний, навыков, умений и опыта:

- компетенций специалиста по КБ широкого профиля;
- знаний об особенностях организации технологических процессов и бизнес-процессов в транспортной отрасли, учитываемых при решении задач обеспечения КБ;
- навыков применения теоретических знаний и междисциплинарных связей;
- компетенций тестирования безопасности компьютерных систем и повышения их защищенности;
- навыков и умений с использованием технологий «виртуальных машин» и свободно распространяемого ПО — web-площадок для тестирования web-уязвимостей;
- опыта участия в олимпиадах, соревнованиях по КБ, в частности, формата *Capture the flag (CTF)*, международных проектах;
- опыта публикационной деятельности.

Эти принципы на протяжении многих лет доказали свою состоятельность и позволили нашим выпускникам реализовать себя в профессиональной сфере. Остановимся подробнее на каждом.

Формирование компетенций специалиста широкого профиля

Действующие образовательные стандарты в области КБ опираются на профессиональные стандарты в следующих областях: «Связь, информационные и ком-

муникационные технологии» и «Обеспечение безопасности». Это определяет требования к выпускникам — специалистам широкого профиля, обладающим компетенциями в области системного анализа, программирования, тестирования, информационных технологий, технической поддержки и администрирования информационно-коммуникационных систем, защиты информации в телекоммуникационных системах и сетях, автоматизации информационно-аналитической деятельности в сфере безопасности компьютерных систем и сетей, защиты информации в автоматизированных системах, технической защиты информации, обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Формирование соответствующих компетенций возможно в ходе изучения широкого спектра дисциплин математического цикла, разносторонней подготовки в области информационных технологий, общей инженерной и узкоспециальной подготовки. Успешное решение задач КБ в транспортной отрасли базируется на знаниях о соответствующих объектах информатизации: автоматизированных информационно-управляющих системах, технологических процессах, бизнес-процессах. Эти разделы также нашли отражение в учебном плане. Выпускающая кафедра «Управление и защита информации» является одной из ведущих в университете в области автоматизации и цифровизации на транспорте. Предполагается расширение элементов образовательной программы, связанных с изучением математического аппарата и практической реализации систем машинного обучения и искусственного интеллекта для решения профессиональных задач.

Формированию междисциплинарных связей, навыков применения теоретических знаний, полученных в рамках одних дисциплин, для решения практических задач способствует реализация стратегии «виртуальной» кафедры, в соответствии с которой к подготовке кадров привлекаются ведущие специалисты с разных кафедр РУТ (МИИТ) и высококвалифицированные специалисты — руководители и (или) работники организаций в сфере КБ, в т. ч. наши выпускники.

Теоретическое обучение подкрепляется практическим в виде лабораторных и практических занятий, большого числа практик. При подготовке специалистов используется материально-техническое обеспечение как выпускающей, так и других кафедр университета.

Формирование компетенций тестирования безопасности компьютерных систем

Авторы подготовили программу дисциплины «Методы анализа управления рисками» и реализовали ее на практике. Программа включает в себя темы, связанные непосредственно с управлением рисками в области КБ, анализом защищенности информационных систем, а именно:

— этические аспекты решения задач обеспечения КБ, в рамках которой определяется взаимосвязь таких элементов КБ, как безопасность, удобство пользования и функциональность, даются классификации хакеров и атак, проводится сравнение таких процедур, как анализ защищенности, тестирование на проникновение, поиск уязвимостей [22];

— *web*-уязвимости — проводится анализ уязвимостей, входящих в список *OWASP TOP-10*, анализируется динамика изменения этого списка;

— рекогносцировка — дается определение понятия, определяются ее цели и роль в тестировании на проникновение, проводится классификация этого действия и средств его реализации;

— сканирование сайтов — определяется понятие «сканирование сайтов» и его роль в анализе защищенности, проводится классификация этого действия и средств его реализации;

— *SQL*-инъекции — рассматриваются методы несанкционированного получения информации из баз данных;

— эксплуатация уязвимостей — проводится классификация уязвимостей и средств их эксплуатации;

— закрепление доступа — определяются цели закрепления доступа, рассматриваются реальные кейсы и инструменты реализации закрепления доступа;

— повышение привилегий — рассматриваются методы и инструменты реализации повышения привилегий в различных операционных системах и их дальнейшая эксплуатация;

— сетевые атаки — классифицируются атаки — перехваты сеансов связи по уровням, рассматриваются методы реализации атак, инструменты перехвата трафика, меры противодействия и выявления;

— безопасность беспроводных сетей — рассматриваются основные способы компрометации таких сетей и методы защиты;

— безопасность мобильных приложений — анализируется безопасность мобильных приложений для операционных систем Android и iOS, изучаются механизмы защиты мобильных устройств;

— бинарные уязвимости — рассматриваются способы обнаружения и устранения уязвимостей программного обеспечения, связанных с переполнением буфера памяти;

— проприетарные протоколы и автоматизированные системы управления технологическими процессами (АСУ ТП) — рассматриваются инструменты оценки безопасности АСУ ТП и их элементов;

— социальная инженерия — дается определение понятия «социальная инженерия», определяются ее цели, типы и роль в тестировании на проникновение, дается психологическое обоснование нейролингвистического программирования, раскрываются тактики и стратегии получения информации у «жертвы», реализация задач через социальные сети, определяются риски социальных се-

тей и кражи личности, демонстрируются методы противодействия социальной инженерии;

- введение в стеганографию, стеганоанализ и форензику (компьютерную криминалистику) — анализируются методы и инструменты сокрытия информации в файлах медиа-контента и других каналах связи;

- введение в криптографию — разбираются основные виды атак на современные алгоритмы хеширования и шифрования;

- подготовка отчетов — обучающиеся знакомятся с основными принципами подготовки отчетов о выполненной работе, позволяющих дать заказчику наиболее полную и хорошо структурированную информацию о действиях, выполненных в целях обеспечения КБ.

Темы, связанные с общей теорией управления рисками, а именно:

- анализ стандартов, регламентирующих управление рисками;

- анализ методов управления рисками, применяемых в различных отраслях экономики — обучающиеся выполняют кейсы по применению этих методов к анализу и управлению отдельными типами рисков КБ.

В ходе изучения дисциплины «Методы анализа управления рисками» выполняется большое количество практических заданий с использованием виртуальных машин и web-площадок (киберполигонов, цифровых двойников, тренажеров) для тестирования web-уязвимостей (например itsecgames.com/, xss-game.appspot.com/, 107.152.36.140:8000/, alexbers.com/sql/). Выпускники университета принимают участие в создании этих инструментов. После решения поставленных задач обучающиеся оформляют отчеты, в которых подробно описывают алгоритм решения задач.

Таким образом, студенты учатся выявлять скрытую информацию, занимаются криптоанализом, анализируют вредоносное программное обеспечение, изучают архитектуру и функционирование компьютерных сетей, овладевают следующими навыками: сбор чувствительной информации о цели, поиск уязвимостей в программном обеспечении и web-сайтах, автоматизация процессов, проведение атаки на компьютерную систему.

Выполнение лабораторной работы «Рекогносцировка» включает в себя получение навыков по применению инструментов поиска поддоменов, определение структуры доменов ВУЗов и выявление уязвимостей, связанных с несовершенством этой структуры.

Выполнение лабораторной работы «Сканирование сайта» включает в себя формирование навыков по применению инструментов сканирования сайтов и выбору настроек этих инструментов в зависимости от поставленных задач с целью получения информации о настройках и состоянии его портов, об используемом программном обеспечении.

Выполнение лабораторной работы «XSS-games» включает в себя получение навыков XSS-инъекции, т. е. тестирования возможности несанкционированного доступа на сайты.

Выполнение лабораторной работы «SQL-инъекции» включает в себя получение навыков тестирования возможности несанкционированного доступа к информации, хранящейся в базах данных.

Выполнение лабораторных работ «Samba» и «Priv.Esc» включает в себя получение навыков тестирования возможности несанкционированного управления удаленной машиной, ее сканирования, выявления уязвимостей и доступа к информации, хранящейся на ней.

Выполнение лабораторной работы «Стеганография» включает в себя получение навыков обнаружения скрытой информации в стегоконтейнерах различной природы (графических, текстовых и аудиофайлах).

В настоящее время множество заданий лабораторного практикума расширяется путем включения задач по стегоанализу, анализу бинарных уязвимостей и безопасности мобильных приложений.

Анализ результатов лабораторного практикума, который предполагает выполнение лабораторных работ по нескольким направлениям и решение нескольких десятков задач по перечисленным темам, включает в себя классификацию результатов выполнения лабораторного практикума по различным признакам: типам выявленных уязвимостей (рис. 1), типам рисков, связанных с выявленными уязвимостями (рис. 2), способам преодоления выявленных уязвимостей и рисков (рис. 3).

В ходе выполнения заданий обучающиеся познакомились почти с 20 типами инструментов самого разного назначения, применяемых для решения задач обеспечения КБ (рис. 4).

Выбор инструментов учащимися был весьма разнообразным. В среднем для каждого типа инструментов рассматривались три конкретные реализации (рис. 5).

Интерес представляет выбор нескольких задач для выполнения из множества. Например, при решении задач сканирования из возможных 87 вариантов флагов 32 человека выбрали только 26 (рис. 3). В среднем каждый обучающийся рассмотрел 6 флагов, из них каждый рассматривался пятью обучающимися. Особой популярностью пользовались флаги, позволяющие исследовать открытые порты для определения информации о службе/версии, определить операционную систему, отслеживать путь к хосту.

Во время лабораторного практикума учащиеся интегрировали знания, полученные по дисциплинам различных циклов, работали с разными видами информации. Применение знаний, полученных в дисциплинах математического цикла, теории информации и управления позволяет находить логические связи между различными уязвимостями, инцидентами и рисками. Владение основными положениями теории управления рисками, а именно знание стандартов и умение применять на практике методы управления рисками, позволили решать задачи анализа и управления рисками КБ, выявленными в ходе выполнения лабораторного практикума (рис. 6).

Рис. 1. Типы выявленных уязвимостей

Рис. 2. Типы рисков, связанных с выявленными уязвимостями

Рис. 3. Способы преодоления выявленных уязвимостей и рисков

Рис. 4. Применение различных типов инструментов в ходе лабораторного практикума

Рис. 5. Использование вариантов реализации инструментов различных типов в ходе лабораторного практикума (1 — язык программирования, 2 — база данных уязвимостей, 3 — криптоаналитический пакет, 4 — пакет для анализа стегоконтейнеров, 5 — эмулятор аппаратного обеспечения, 6 — инструменты Windows, 7 — web-площадка для тестирования web-уязвимостей, 8 — загрузчик текста, 9 — обработчик изображений, 10 — интерпретатор, 11 — видео- и аудиоплеер, 12 — компилятор, 13 — декодер, 14 — реверс текста, 15 — онлайн-ресурс, 16 — перебор паролей, 17 — создание, тестирование и использование эксплоитов, 18 — сканер IP-сетей, 19 — перечисление поддоменов web-сайта, 20 — тип «Поисковая система, 21 — HEX-редактор, 22 — анализатор спектра, 23 — операционная система)

Взаимодействие кафедры с компанией, которая напрямую решает задачи информационной безопасности, позволяет восполнить нехватку практического опыта у студентов. Они получают доступ к заданиям, которые моделируют реальные ситуации и кейсы.

Методика позволяет дать более широкое представление о направлениях КБ, выделить из них интересные для студентов и детально показать, чем занимается то или иное направление, решить множество задач, возникающих в повседневной жизни. Такой опыт поможет специалистам чувствовать себя более уверенно в своей области, находить решения в сложных ситуациях, даст хорошую базу для дальнейшего развития.

Среди прослушавших данный учебный курс проводились опросы. Было выявлено, что большинство теоретических знаний получило практическое под-

Рис. 6. Пример применения метода «Анализ дерева неисправности» (FTA) для анализа уязвимости «Разглашение конфиденциальных данных»

крепление в форме решения разнообразных задач. Обучающиеся смогли детально понять направления, на которые разделяется КБ, и впоследствии попасть на стажировки и курсы в компании, работающие в этой сфере.

Участие студентов в олимпиадах, соревнованиях, международных проектах и публикационной деятельности

Отчеты учащихся о результатах индивидуальных заданий по дисциплине «Методы анализа управления рисками», выполненных в весеннем семестре 2019–2020 учебного года и содержащие презентации, визуальные элементы и анализ статистики, нашли применение в учебном процессе. Они размещены на сервере

дистанционного обучения Института транспортной техники и систем управления РУТ (МИИТ), который дает доступ к широкому спектру методических материалов и электронных курсов, разработанных преподавателями университета.

Примерами такого эффективного использования результатов (в т. ч. выпускной квалификационной работы) стали издания, посвященные различным проблемам КБ [23–27].

Обучающиеся активно участвуют в олимпиадах по информационной и компьютерной безопасности, соревнованиях формата СТФ, конференциях и тематических форумах (рис. 7), печатаются в научных изданиях [28–31]. Студенты активно сотрудничают с Университетом прикладных наук в немецком городе Аугсбурге.

Заключение

Практическое воплощение сформулированных в статье принципов позволит реализовать подготовку востребованных на рынке труда специалистов КБ широкого профиля, которые:

— умеют применять фундаментальные знания, чтобы выявлять и выбирать пути решения профессиональных проблем и задач, анализировать результаты этого решения;

Рис. 7. Обучающиеся РУТ (МИИТ) на одном из форумов

— владеют навыками тестирования компьютерных систем с использованием современного программного, информационного и технического обеспечения в рамках правового поля и норм профессиональной этики;

— обладают знаниями об особенностях организации технологических процессов и бизнес-процессов в транспортной отрасли;

— имеют фундамент для профессионального роста и реализации концепции непрерывного образования, предполагающих развитие не только в прикладной, но и в научной, международной и педагогической сферах.

Эффективное использование всех возможностей университета с целью реализации крайне важной для транспортной отрасли образовательной программы по компьютерной безопасности, тесная связь с производством («предметной областью»), близкое знакомство с объектами информатизации, безопасность которых предстоит обеспечивать — вот отличительные черты подготовки кадров в РУТ (МИИТ).

В поддержку сказанного стоит отметить, что темы выпускных квалификационных работ учащихся отражают многообразие объектов информатизации не только в транспортной, но и в других отраслях экономики, и современных методов, применяемых для обеспечения информационной безопасности, а также технических и программных средств. Выполнение ВКР предполагает построение соответствующих математических моделей или применение методов системного анализа.

Выпускники востребованы в различных сферах экономики, проходят практику и трудоустраиваются в такие организации, как ГВЦ ОАО «РЖД», «Информзащита», «Лаборатория Касперского», ОАО «НИИАС», «ИБТранс», ООО «СЕК-Консалт Сервисез», другие коммерческие и государственные структуры.

По информации Всемирной организации здравоохранения, за время пандемии число кибератак возросло в несколько раз [32], что способствует повышению востребованности выпускников специальности КБ на рынке труда. Это подтверждают и данные сайтов по поиску работы и сотрудников (например *hh.ru*). Согласно этим данным, количество вакансий превышает число бюджетных мест, на которое осуществлялся набор в вузы в этом году на соответствующие специальности. Можно предполагать, что в предстоящие годы спрос на специалистов в области КБ будет расти. Требования к их квалификации будут становиться все более высокими. Следовательно, высшие учебные заведения должны соответствовать новым вызовам и постоянно совершенствовать ОП. Изложенные в статье принципы позволяют это воплотить, что подтверждается многолетней практикой подготовки кадров для обеспечения КБ транспортной отрасли.

Библиографический список

1. Огородников Е. Кибербезопасность «Российских железных дорог» обеспечат отечественные разработчики [Электронный ресурс]. – 2020. Режим доступа: <https://expert.ru>.

- ru/2020/06/19/kiberbezopasnost-rossijskih-zheleznih-dorog-obespechat-otchestvennyie-razrabotchiki/
2. Покровская И. Защитники информации [Электронный ресурс]. – 2020. Режим доступа: <https://gudok.ru/newspaper/?ID=1504600&archive=2020.05.21>
 3. Белова И. В. Совершенствование подготовки специалистов по прикладной информатике в области информационной безопасности (уровень среднего профессионального образования) // Казанская наука. – 2012. – № 9. – С. 191–193.
 4. Анурьева М. С. Современная система образования в области информационной безопасности в Российской Федерации // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2018. – Т. 23. – № 173. – С. 111–120.
 5. Анурьева М. С. Научный базис сравнительного анализа программ подготовки специалистов по информационной безопасности в разных странах // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2018. – Т. 23. – № 171. – С. 90–97.
 6. Crick T., Davenport J., Irons A., Prickett T. A UK Case Study on Cybersecurity Education and Accreditation // Conference: 2019 IEEE Frontiers in Education Conference (FIE). – October 2019. – DOI: 10.1109/FIE43999.2019.9028407.
 7. Martti Lehto. Cyber security capacity building – cyber security education in Finnish universities // Proceedings of the 19th European Conference on Cyber Warfare and Security. – UK. – 2020. – DOI: 10.34190/EWS.20.112.
 8. Kessler G. C., Ramsay J. D. A Proposed Curriculum in Cybersecurity Education Targeting Homeland Security Students // Proceedings of the 47th Hawaii International Conference on System Sciences. – HI. – 2014. – Pp. 4932–4937. – DOI: 10.1109/HICSS.2014.605.
 9. Frankie E Catota, M Granger Morgan, Douglas C Sicker Cybersecurity education in a developing nation: the Ecuadorian environment // Journal of Cybersecurity, Volume 5, Issue 1, 2019, tyz001, [Электронный ресурс]. – 2020. Режим доступа: <https://doi.org/10.1093/cybsec/tyz001>.
 10. Furnell S., K M., Piper F., E C., H C., Ensor C. A National Certification Programme for Academic Degrees in Cyber Security // Information Security Education – Towards a Cybersecure Society. WISE 2018. IFIP Advances in Information and Communication Technology, Springer, Cham. – 2018. – Vol 531. [Электронный ресурс]. – 2020. Режим доступа: https://doi.org/10.1007/978-3-319-99734-6_11.
 11. Мовчан И. Н. Проблемы подготовки специалистов в области информационной безопасности // Открытое образование. – 2013. – № 5 (100). – С. 78–80.
 12. Козлов О. А., Симонова И. В., Бочаров М. И. Модели обучения информационной безопасности // Материалы международной научно-практической конференции «Инновации на основе информационных и коммуникационных технологий». – 2013. – Т. 1. – С. 28–30.
 13. Huang Z., Shen C., Doshi S., Thomas N., Duong H. Cognitive Task Analysis Based Training for Cyber Situation Awareness // Information Security Education Across the Curriculum. WISE 2015. IFIP Advances in Information and Communication Technology. – Springer, Cham. – 2015. – Vol. 453. [Электронный ресурс]. – 2020. Режим доступа: https://doi.org/10.1007/978-3-319-18500-2_3.
 14. Futch L., Van Niekerk J. Towards a Pervasive Information Assurance Security Educational Model for Information Technology Curricula // Information Assurance and Security Education and Training. – Pp. 164–171.
 15. Švábenský V., Vykopal J., Celeda P. What Are Cybersecurity Education Papers About? – A Systematic Literature Review of SIGCSE and ITiCSE Conferences. – 2019. [Электронный ресурс]. – 2020. Режим доступа: <https://arxiv.org/pdf/1911.11675.pdf>

16. Moore E., Likarish D. (2015) A Cyber Security Multi Agency Collaboration for Rapid Response that Uses AGILE Methods on an Education Infrastructure. In: Bishop M., Miloslavskaya N., Theocharidou M. (eds) Information Security Education Across the Curriculum. WISE 2015. IFIP Advances in Information and Communication Technology, vol 453. Springer, Cham. https://doi.org/10.1007/978-3-319-18500-2_4.
17. Bada M., Nurse J.R. C. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs) // Information and Computer Security. – Vol. 27. № 3. – Pp. 393–410. – DOI: 10.1108/ICS-07-2018-0080.
18. Charalambos K. Cyber-Physical Systems Security Education Through Hands-on Lab Exercises // IEEE Design & Test. – 2020. – Pp. 1–1. – DOI: 10.1109/MDAT.2020.3005365.
19. Davidson A., Javier de La Puente Martinez, Huber M. A SWOT Analysis of Virtual Laboratories for Security Education // Information Assurance and Security Education and Training. – Pp. 233–240.
20. Sauer F., Niedermaier, M., Kießling S., Merli D. LICSTER – A Low-cost ICS Security Tested for Education and Research.. (2019. [Электронный ресурс]. – 2020. Режим доступа: <https://arxiv.org/pdf/1910.00303.pdf>.
21. Киберучения на «цифровом двойнике» инфраструктуры: оценка реальных рисков для бизнеса [Электронный ресурс]. – 2020. Режим доступа: <https://www.ptsecurity.com/ru-ru/research/knowledge-base/kiberucheniya-na-cifrovom-dvojnike-infrastruktury-ocenka-realnyh-riskov-dlya-biznesa>.
22. Bustard J.D. Improving Student Engagement in the Study of Professional Ethics: Concepts and an Example in Cyber Security // Sci Eng Ethics 24. – 2018. – Pp. 683–698. [Электронный ресурс]. – 2020. Режим доступа: <https://doi.org/10.1007/s11948-017-9904-4>.
23. Изычева А. В., Сидоренко В. Г. Стеганографические методы защиты информации: учебное пособие. – М.: МИИТ, 2017. – 76 с.
24. Воронина Е. Г., Сидоренко В. Г. Генераторы случайных чисел: учебное пособие. – М.: РУТ (МИИТ), 2018. – 80 с.
25. Арцыбашева А. А., Козлов А. А., Сидоренко В. Г. Анализ подлинности изображения: учебное пособие. – М.: РУТ (МИИТ), 2018. – 106 с.
26. Скоробогатова Н. Н., Сидоренко В. Г. Аспекты информационной безопасности: учебное пособие. – М.: РУТ (МИИТ), 2018. – 80 с.
27. Замолоцких В. С., Сидоренко В. Г. Применение теории графов для анализа социальных сетей: учебное пособие. – М.: РУТ (МИИТ), 2020. – 74 с.
28. Замолоцких В. С., Сидоренко В. Г. Киберугрозы в социальных сетях // Информатизация образования и науки. – 2020. – № 4 (48). – С. 66–75.
29. Водясов А. Е., Сидоренко В. Г. Анализ проблемы обеспечения безопасности смарт-контрактов // Сборник материалов II международной научно-практической конференции «Цифровая трансформация в экономике транспортного комплекса. Развитие цифровых экосистем: наука, практика, образование». – М.: РУТ (МИИТ), 2020. – С. 66–70.
30. Кирюхин Д. М. Анализ проблематики реализации требований по информационной безопасности к объектам критической информационной инфраструктуры Российской Федерации в транспортной отрасли // Сборник материалов II международной научно-практической конференции «Цифровая трансформация в экономике транспортного комплекса. Развитие цифровых экосистем: наука, практика, образование». – М.: РУТ (МИИТ), 2020. – С. 148–151.
31. Павлов Н. А. Биометрические методы аутентификации: основные понятия, механизмы, надежность и актуальность в сфере транспорта // Сборник материалов II-ой международной научно-практической конференции «Цифровая трансформация в экономике

транспортного комплекса. развитие цифровых экосистем: наука, практика, образование». – М.: РУТ (МИИТ), 2020. – С. 261–266.

32. ВОЗ сообщила о росте кибератак во время пандемии в пять раз [Электронный ресурс]. – 2020. Режим доступа: <https://lenta.ru/news/2020/04/24/cyber/>.

A. E. Vodyasov

D. M. Kiryukhin

G. V. Sidorenko, Dr. Sci. in Engineering

SEC-CONSULT SERVICES, LLC

Department of Control and Information Security,

Russian University of Transport, Moscow

EXPERIENCE IN TRAINING PERSONNEL TO ENSURE THE COMPUTER SECURITY OF THE TRANSPORT INDUSTRY

In the context of the pandemic, the role of computer security specialists in solving the problems of uninterrupted operation of transport enterprises has increased many times. The article is devoted to summing up and analyzing the experience accumulated in the RUT (MIIT) for 20 years of training specialists in the specialty "Computer Security", determining the prospects for the development of the educational program. The article presents a methodology for using freely distributed software created by the authors of the article in the learning process in cases where it is impossible or unsafe on real objects. The main advantage of this technique is that it takes into account the experience gained by specialists in solving real cases, allows you to reproduce real system vulnerabilities without harming real systems for training purposes, makes it possible to diagnose these vulnerabilities, exploit them, choose and compare different ways to remove them from the system. The article contains an analysis of publications devoted to the experience of training personnel in the specialty "Computer Security" in different countries using various tools. The article provides an overview of the educational program and formulates the principles that form the basis of training at our university, demonstrates examples of the use of digital doubles in the learning process, focuses on the formation of interdisciplinary connections, skills of applying theoretical knowledge to solve practical problems and analyze the results obtained. The review of the subjects of the discipline "Methods of risk management analysis", statistical analysis of the results of the implementation of the methodology developed by the authors in practice, and their graphical interpretation is carried out. Examples of the application of risk theory to solving computer security problems are given. The article contains examples of students' participation in research activities, the creation of methodological support for the relevant educational program, and various events outside the university.

Computer security, training, digital double, vulnerability, risk

DOI: 10.20295/2412-9186-2021-7-2-315-335

References

1. Ogorodnikov E. Cybersecurity of "Russian Railways" will be provided by domestic developers – 2020. <https://expert.ru/2020/06/19/kiberbezopasnost-rossijskih-zheleznnyih-dorog-obe-spechat-otechestvennyie-razrabotchiki/>
2. Pokrovskaya, I. Defenders of the information. – 2020. <https://gudok.ru/newspaper/?ID=1504600&archive=2020.05.21>

3. Belova I. V. Improving the training of specialists in applied computer science in information security (level of secondary vocational education) // *Kazan Science*. – 2012. – № 9. – Pp. 191–193.
4. Anureva M. S. Modern system of education in the field of information security in the Russian Federation // *Tambov university review: series humanities*. – 2018. – T. 23. – № 173. – Pp. 111–120.
5. Anureva M. S. Research basis of comparative analysis of specialists' preparation programs in information security in different countries // *Tambov university review: series humanities*. – 2018. – T. 23. – № 171. – Pp. 90–97.
6. Crick T., Davenport J., Irons A., Prickett T. A UK Case Study on Cybersecurity Education and Accreditation // *Conference: 2019 IEEE Frontiers in Education Conference (FIE)*. – October 2019. – DOI: 10.1109/FIE43999.2019.9028407.
7. Martti Lehto. Cyber security capacity building -cyber security education in Finnish universities Cyber security capacity building – cyber security education in Finnish universities // *Proceedings of the 19th European Conference on Cyber Warfare and Security*. – UK. – 2020. – DOI: 10.34190/EWS.20.112.
8. Kessler G. C., Ramsay J. D. A Proposed Curriculum in Cybersecurity Education Targeting Homeland Security Students // *Proceedings of the 47th Hawaii International Conference on System Sciences*. – HI. – 2014. – Pp. 4932–4937. – DOI: 10.1109/HICSS.2014.605.
9. Frankie E. Catota, M. Granger Morgan, Douglas C. Sicker. Cybersecurity education in a developing nation: the Ecuadorian environment // *Journal of Cybersecurity*, Volume 5, Issue 1, 2019, tyz001. <https://doi.org/10.1093/cybsec/tyz001>.
10. Furnell S., K M., Piper F., E C., H C., Ensor C. A National Certification Programme for Academic Degrees in Cyber Security // *Information Security Education – Towards a Cybersecure Society*. WISE 2018. IFIP Advances in Information and Communication Technology, Springer, Cham. – 2018. – Vol 531. https://doi.org/10.1007/978-3-319-99734-6_11.
11. Movchan I. N. Problems of training professionals in the field of information security // *Open education*. – 2013. – № 5 (100). – Pp. 78–80.
12. Kozlov O. A., Simonova I. V., Bocharov M. I. Models of information security training // *Proceedings of the international scientific and practical conference “Innovations based on Information and communication technologies»*. – 2013. – T. 1. – Pp. 28–30.
13. Huang Z., Shen CC., Doshi S., Thomas N., Duong H. Cognitive Task Analysis Based Training for Cyber Situation Awareness // *Information Security Education Across the Curriculum*. WISE 2015. IFIP Advances in Information and Communication Technology. – Springer, Cham. – 2015. – Vol. 453. – 2020. https://doi.org/10.1007/978-3-319-18500-2_3.
14. Fitcher L., Van Niekerk J. Towards a Pervasive Information Assurance Security Educational Model for Information Technology Curricula // *Information Assurance and Security Education and Training*. – Pp 164–171.
15. Švábenský V., Vykopal J., Celeda P. What Are Cybersecurity Education Papers About? – A Systematic Literature Review of SIGCSE and ITiCSE Conferences. – 2019. – 2020. <https://arxiv.org/pdf/1911.11675.pdf>
16. Moore E., Likarish D. (2015) A Cyber Security Multi Agency Collaboration for Rapid Response that Uses AGILE Methods on an Education Infrastructure. In: Bishop M., Miloslavskaya N., Theodoridou M. (eds) *Information Security Education Across the Curriculum*. WISE 2015. IFIP Advances in Information and Communication Technology, vol 453. Springer, Cham. https://doi.org/10.1007/978-3-319-18500-2_4.
17. Bada M., Nurse, J. R. C. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs) // *Information and Computer Security*. – Vol. 27. № 3. – Pp. 393–410. – DOI: 10.1108/ICS-07-2018-0080.

18. Charalambos K. Cyber-Physical Systems Security Education Through Hands-on Lab Exercises // IEEE Design & Test. – 2020. – Pp. 1–1. – DOI: 10.1109/MDAT.2020.3005365.
19. Davidson A., Javier de La Puente Martinez, Huber M. A SWOT Analysis of Virtual Laboratories for Security Education // Information Assurance and Security Education and Training. – Pp. 233–240.
20. Sauer F., Niedermaier, M., Kießling S., Merli D. LICSTER – A Low-cost ICS Security Testbed for Education and Research. – 2019. <https://arxiv.org/pdf/1910.00303.pdf>.
21. Cyber-learning on the” digital twin “ of infrastructure: assessing real business risks. – 2020. <https://www.ptsecurity.com/ru-ru/research/knowledge-base/kiberucheniya-na-cifrovom-dvojnike-infrastruktury-ocenka-realnyh-riskov-dlya-biznesa/>
22. Bustard, J. D. Improving Student Engagement in the Study of Professional Ethics: Concepts and an Example in Cyber Security // Sci Eng Ethics 24. – 2018. – Pp. 683–698. <https://doi.org/10.1007/s11948-017-9904-4>.
23. Izycheva A. V., Sidorenko V. G. Steganographic methods of information security: Training manual. – M.: RUT (MIIT), 2017. – 76 p.
24. Voronina E. G., Sidorenko V. G. Random number generators: Training manual. – M.: RUT (MIIT), 2018. – 80 p.
25. Artsybasheva A. A., Kozlov A. A., Sidorenko V. G. Analysis of image authenticity: Training manual. – M.: RUT (MIIT), 2018. – 106 p.
26. Skorobogatova N. N., Sidorenko V. G. Aspects of information security: Training manual. – M.: RUT (MIIT), 2018. – 80 p.
27. Zamolotskikh V. S., Sidorenko V. G. Application of graph theory for social network analysis: Training manual. – M.: RUT (MIIT), 2020. – 74 p.
28. Zamolotskikh V. S., Sidorenko V. G. Cyber threats in social networks // Informatization of education and science. – 2020. – № 4 (48). – Pp. 66–75.
29. Vodyasov A. E. Sidorenko G. V. Smart contract security problem review // Proceedings of the II-th International Scientific and Practical Conference «Digital transformation in the economy of the transport complex. Development of digital ecosystems: science, practice, education». – M.: RUT (MIIT), 2020. – 66–70 p.
30. Kiryukhin D. M. Analisis of the problem of implementation of requirements for information security to objects of critical information infrastructure of the russian federation in the transport industry // Proceedings of the II-th International Scientific and Practical Conference «Digital transformation in the economy of the transport complex. Development of digital ecosystems: science, practice, education». – M.: RUT (MIIT), 2020. – 148–151 p.
31. Pavlov N. A. Biometric methods of authentificaion: basic concepts, mechanisms, reliability and relevance in transport // Proceedings of the II-th International Scientific and Practical Conference «Digital transformation in the economy of the transport complex. Development of digital ecosystems: science, practice, education». – M.: RUT (MIIT), 2020. – 261–266 p.
32. WHO reported a five-fold increase in cyber attacks during the pandemic. – 2020. <https://lenta.ru/news/2020/04/24/cyber/>.

*Статья представлена к публикации членом редколлегии
профессором Л. А. Барановым*

Поступила в редакцию 17.12.2020, принята к публикации 10.02.2021

ВОДЯСОВ Алексей Евгеньевич — технический директор ООО «СЕК-КОНСАЛТ
СЕРВИСЭЗ»
lexadin@yandex.ru

КИРЮХИН Дмитрий Максимович — эксперт по информационной безопасности
ООО «СЕК-КОНСАЛТ СЕРВИСЕЗ»
dimonkm4red@gmail.com

СИДОРЕНКО Валентина Геннадьевна — доктор технических наук, профессор
кафедры «Управление и защита информации» РУТ (МИИТ)
valenfalk@mail.ru

© Водясов А. Е., Кирюхин Д. М., Сидоренко В. Г., 2021