ТРАНСПОРТНАЯ БЕЗОПАСНОСТЬ В ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАНИИ

УДК 372.8:378:656

© Сидоренко Валентина Геннадьевна,
доктор технических наук, профессор,
Российский университет транспорта (МИИТ)
valenfalk@mail.ru

© Логинова Людмила Николаевна,
кандидат технических наук, доцент,
Российский университет транспорта (МИИТ)
ludmilanv@mail.ru

Современные аспекты образовательной деятельности для обеспечения информационной безопасности транспортной отрасли

Аннотация. В современных условиях специалисты в области компьютерной безопасности и защиты информации востребованы особенно для обеспечения бесперебойной работы транспортной отрасли. Статья посвящена анализу аспектов образовательной деятельности кафедры «Управление и защита информации» РУТ (МИИТ), которая готовит специалистов по специальности «Компьютерная безопасность». Дан обзор образовательной программы, сформулированы принципы, положенные в основу подготовки специалистов по защите информации в РУТ (МИИТ). Продемонстрированы темы, которые студенты изучают в рамках образовательной программы.

Ключевые слова: компьютерная безопасность; защита информации; информационная безопасность; подготовка кадров; уязвимость; риск

© Valentina G. Sidorenko,
Doctor of Technical Sciences, professor,
Russian University of Transport
valenfalk@mail.ru

© Lyudmila N. Loginova,
Candidate of Technical Sciences, associate professor,
Russian University of Transport
ludmilanv@mail.ru

Current facets of educational activities to ensure information security of the transport industry

Abstract. In modern conditions, there is a great need in specialists working in the field of cyber security and information protection, especially to ensure the smooth operation of the transport industry. The current paper deals with the analysis of facets of educational activities of the department “Information Management and Protection” of RUT (MIIT), which trains specialists of “Cyber security”. There has been presented an overview of the educational program. There has been formulated the principles underlying the training of cyber security specialists in RUT (MIIT). There have been demonstrated the themes which are studied as part of the educational program.

Keywords: cyber security; information protection; information security; staff training; vulnerability; risk.

В условиях повсеместной цифровизации, интеллектуализации и, как следствие, роста объемов обрабатываемых данных вопрос защиты данных, их собственников и пользователей встает на первое место. Несмотря на широкое освоение множества базовых информационных технологий, лишь небольшая часть компаний способна верно выстраивать бизнес-процессы, грамотно выделять ресурсы и оценивать риски, связанные с информационной безопасностью. Специалисты по защите информации и компьютерной безопасности становятся наиболее востребованными в условиях сложившейся геополитической, экономической и общественной обстановки. Государственные высшие учебные заведения, частные образовательные организации наблюдают повышенный интерес абитуриентов к получению знаний и навыков по защите информации и компьютерной безопасности. В связи с этим модернизация образовательных программ в области защиты информации и компьютерной безопасности на основе накопленного опыта и последних достижений в области науки и техники является актуальным вопросом.

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 том числе ОАО «РЖД», активно внедряются новые информационные технологии, что повышает актуальность решения задач компьютерной безопасности.

Выпускники, как будущие специалисты широкого профиля, должны обладать 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, разносторонней подготовки в области информационных технологий, общей инженерной и узкоспециальной подготовки. Успешное решение задач компьютерной безопасности в транспортной отрасли базируется на знаниях о соответствующих объектах информатизации: автоматизированных информационно-управляющих системах, технологических процессах, бизнес-процессах. Выпускающая кафедра «Управление и защита информации» является одной из ведущих в университете в области автоматизации и цифровизации на транспорте. В реализуемой образовательной программе уделяется внимание всем аспектам информационной безопасности, защиты информации и компьютерной безопасности.

Большое внимание в процессе подготовки уделяется изучению методов и средств командной работы, подготовке отчетной документации в соответствии с общепринятыми стандартами.

Проводить объективную оценку уровня подготовки студентов позволяет выполнение командных работ по дисциплине «Проектная деятельность», реализация курсовых работ по изучаемым дисциплинам, защита выпускной квалификационной работы, тематика которых отражает все разнообразие деятельности специалистов в области информационной безопасности, компьютерной безопасности и защиты информации применительно к различным отраслям экономики.

Несомненно, современные специалисты в области информационной безопасности, защиты информации и компьютерной безопасности должны обладать актуальными знаниями о наиболее значимые уязвимостях и угрозах безопасности веб-приложением. Выпускники должны уметь оценивать существующие уязвимости, причины их возникновения и возможный ущерб. Одной из задач при обучении будущих специалистов области информационной безопасности, защиты информации и компьютерной безопасности является расширение множества используемых специалистами популярных бесплатных инструментов с открытым кодом для пентестинга (тестирования на проникновение), который автоматически выявляет основные классы *SQL*-инъекций: *SQLMap*, *jSQL Injection*, *BBQSQL*, *NoSQLMap*, *WebCruiser, Arachni*. На кафедре «Управление и защита информации» (УиЗИ) РУТ (МИИТ) студенты изучают функционал широкого спектра инструментов, а также используют эти инструменты при выполнении дипломного

проектирования, принимают участие в конференциях с темами исследований, посвященными *SQL*-инъекциям.

В рамках проведения работы над выпускной работой студенты кафедры знакомятся с технологиями блокчейн, выполняют дипломные проекты для решения вопросов повышения защищенности распределенной финансовой организации, основанной на использовании технологии блокчейн.

Одной из актуальных задач в области информационной безопасности в системах интеллектуального управления является мониторинг безопасности объектов (МБО), который должен обеспечивать формирование доверенных маршрутов и отслеживание информационных потоков, контроль подключений внешних объектов или субъектов, конфигурирование маршрутизаторов и взаимодействие с коммутаторами, что для транспортной системы является исключительно важным, так как транспорт относится к критически важным сферам функционирования отраслей экономики и должен обеспечивать безопасную перевозку пассажиров и грузов.

В нормативной области безопасность регулируется Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а конкретные требования указаны в приказе ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Таким образом, основная задача мониторинга безопасности объектов состоит в контроле подключений к критически важным объектам инфраструктуры предприятия и управлении доверенными маршрутами сети в режиме реального времени, что позволит своевременно реагировать и предотвращать несанкционированные действия внешних пользователей, и, как следствие, исключить возможность хищения данных, а также нарушения работоспособности серверов. Студенты кафедры принимают участие в повышении защищенности локальной сети железнодорожного предприятия путем разработки МБО-анализаторов (модели мониторинга объектов внешних атак).

Эффективная работа, связанная с анализом и обработкой информации, невозможна без использования компьютерных сетей. Сети как государственных, так и коммерческих компаний, в Интернет обеспечивают доступ к базам данных. Технология удаленного доступа предполагает решения различных видов функциональных задач компании или бизнес-процессов с использованием глобальной сети Интернет. При этом процесс организации удаленного доступа на сегодняшний день должен учитывать новые общественные условия. Вопросы разработки системы защиты удаленного доступа и конфигурирования виртуальной частной сети (*VPN*) на основе актуальных

криптографических протоколов выходят на первые места. Студенты кафедры УиЗИ рассматривают методы реализации удаленного доступа пользователей к корпоративной сети; проводят анализ угроз и *VPN*-протоколов для обеспечения информационной безопасности; разрабатывают и настраивают конфигурации защищенного *VPN*-туннеля между узлами компьютерной сети.

Это лишь часть направлений разносторонних исследований, проводимых студентами.

Реализация важнейшей в настоящее время образовательной программы по защите информации и компьютерной безопасности, тесная связь с объектами информатизации, рассмотрение актуальных вопросов защиты информации и компьютерной безопасности являются отличительной чертой подготовки кадров для обеспечения безопасности транспортной отрасли.