ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ГЕОДЕЗИИ

Черняева А.А., Сухова Е.Р.
студентки 4 курса ГБПОУ ВО «Воронежский государственный профессионально-педагогический колледж», г. Воронеж, Российская Федерация
Научный руководитель – Денисова О.А., преподаватель

В данном разделе рассматривается актуальная проблема создания новой специальности по подготовке специалистов в области геодезии и картографии так как эта область требует безопасности программного обеспечения. На текущий момент не существует самостоятельных специалистов, сочетающих в себе все необходимые знания и компетенции в данной области. Востребованность специалистов по безопасности программного обеспечения обусловлена развитием информационных и автоматизированных систем, к которым предъявляются высокие требования по стойкости и корректности действий.

Профессиональная область деятельности, связанная с защитой информации, как известно, весьма широка. Поэтому базовый уровень подготовки специалистов по инженерно-техническим кадрам в информационной безопасности просто физически не может охватить весь спектр возможных профессиональных задач и областей деятельности, в связи с чем возникает потребность в дальнейшем профессиональном развитии и более узкой специализации профильных специалистов.

Данное направление является сравнительно молодое, поэтому в нём ещё не сформировались все компетентностные сегменты. В тоже время, индустрия информационных технологий развивается весьма стремительно. И если в 1980-е годы области применения ЭВМ представлялись преимущественно в вычислительных задачах, то в настоящее время вычислительная техника широко используется в управлении, финансах, сборе, хранении и обработке информации, системах жизнеобеспечения, системах искусственного интеллекта.

Соответственно, кардинально изменились представления о рисках, связанных с применением вычислительных средств и программного обеспечения. Некорректная реакция автоматизированных систем управления и жизнеобеспечения может повлечь за собой непоправимые последствия.

Ожидается, что в течение ближайшего десятилетия начнется активное развитие беспилотного транспорта. Хотя уже и сейчас бортовые системы автомобилей отрабатывают множество состояний и корректируют действия водителя для предотвращения опасных ситуаций, а бортовые системы новейших самолетов способны контролировать положение судна в пространстве, вести по курсу, и даже брать на себя основные функции при взлёте и посадке.

К программной части геодезических систем должны предъявляться жесточайшие требования по корректности работы и защищённости от внешних деструктивных воздействий, в том числе от попыток вмешательства в их алгоритмы работы.

К сожалению, устоявшиеся принципы разработки программного обеспечения, когда выпуск фактически не полноценного программного продукта, с ошибками, недоработками, поверхностным тестированием, и с последующим выпуском множества обновлений – не отвечают указанным требованиям. Термин «уязвимости программного обеспечения» хорошо известен IT-специалистам, сюда входят и упущения разработчиков, и не декларированные возможности, и некорректности в программном коде. Самое печальное здесь то, что даже по истечении многих лет массового использования программного продукта, при регулярной поддержке разработчика и выпускаемых обновлениях, в программных системах всё равно продолжают обнаруживаться новые уязвимости. Пользователям и эксплуататор программных систем зачастую недоступна полная документация на программные продукты, детализирующая их алгоритмы и методы обработки информации, а многие системные действия, как создание

служебных записей, получение доступа к файлам и ресурсам – просто скрыты и непрозрачны. Такова модель функционирования современных программных систем, и таковы маркетинговые принципы их разработчиков.

Самостоятельных специалистов, которые целенаправленно занимались бы формированием стратегии разработки безопасного программного обеспечения, полноценным тестированием, экспертизой, фактически не готовится. Частично этим занимаются специалисты по безопасности автоматизированных систем, информационной безопасности, программисты, представители иных смежных профессий.

В то же время инженерно-техническим специалистам по безопасности программного обеспечения должны иметь обособленный комплекс знаний и умений, который в настоящее время полностью не формируется ни в одной из смежных областей. Здесь требуются знания по операционным системам, программированию, теории алгоритмов, криптографии, протоколам и интерфейсам, методам и системам тестирования, автоматизации, инженерии, документоведению, управлению, праву.

Можно заключить, что одной из наиболее востребованных профессий будущего станет профессия специалиста по безопасности программного обеспечения, и в настоящее время необходимо сформировать комплекс компетенций и требований, которым должен будет удовлетворять специалист данного профиля.

Литература

1.Сиротский А.А. Информационная безопасность личности и защита персональных данных в современной коммуникативной среде // Технологии техносферной безопасности, 2013. – № 4 (50). – С. 18.

2.Сиротский А.А. Совершенствование методов обеспечения безопасности при авторизации в системах дистанционного банковского обслуживания // Технологии техносферной безопасности, 2013. – № 6 (52). – С. 14.

3.Сиротский А.А. Содержание и методология преподавания дисциплины «теория автоматов и формальных языков» при подготовке IT-специалистов // В сборнике: Преподавание информационных технологий в Российской Федерации. Материалы Десятой открытой Всероссийской конференции. Москва, Издательство МГУ, 2012. – С. 419-421.

4.Сиротский А.А. Распределенные системы. Организация и типология // Техника машиностроения, 2012. – № 2 (82). – С. 34-37.

5.Баранова Е.К., Сиротский А.А. Особенности подготовки бакалавров по направлению «информационная безопасность» в широкопрофильном социальном университете // Информационное противодействие угрозам терроризма, 2015. – № 25. – С. 31-37.

6.Сиротский А.А. Особенности преподавания дисциплины «физические основы защиты информации» // В сборнике: Преподавание информационных технологий в Российской Федерации. Материалы Одиннадцатой открытой Всероссийской конференции. ВГУ, Воронеж, 2013. – С. 280-282.

7.Сиротский А.А., Мироничев А.Г. Windows XP как потенциальная уязвимость в российском бизнесе // // В сборнике: Современные проблемы информационной безопасности и программной инженерии. Сборник избранных статей научного семинара №1(6) кафедры информационной безопасности и программной инженерии. РГСУ, Москва, Издательство ООО «Сам полиграфист», 2014. – С. 84-87.

ПРОГРАММНЫЙ МОДУЛЬ ДЛЯ УПРАВЛЕНИЯ ТРЕХКООРДИНАТНЫМ ФРЕЗЕРНЫМ ЧПУ-СТАНКОМ

Шлепоченко М.А.

учащийся 3 курса Оршанского колледжа ВГУ имени П.М. Машерова, г. Орша, Республика Беларусь

Научный руководитель – Романцов Д.Ю., магистр технических наук

Нынешнее развитие индустрии требует постоянного совершенствования производства и высокой точности. Станок с числовым программным управлением (ЧПУ) является основным производственным модулем современной индустрии. Данные станки используются как для автоматизации мелкосерийного или штучного производства, так и для крупных серий. Изготовление прототипов печатных плат обычно требует достаточно большого