комплексных задач. Необходимо подчеркнуть, что на данном этапе создания электронного правительства государственная власть, как никогда, нуждается в тех эффективных управленцах, которым можно будет доверить в большей или меньшей степени часть своих функций. Следует отметить, что знаний по базовым информационным технологиям и умения работать с соответствующим инструментарием недостаточно для эффективной деятельности гражданина и профессионала в информационном обществе.

Особенностью современного этапа развития белорусского государства является цифровая трансформация как общегосударственная задача, которая становится эффективной при условии, если ее принципы и технологии внедряются на всех уровнях государственного управления. В нашем исследовании мы отмечаем, что эффективность цифровой трансформации и во многом зависит от компетенций в этой сфере управленческого аппарата всех уровней управления.

В своем исследовании мы исходим из того, что компетентностные уровни государственных управленцев могут формироваться посредством образовательного процесса в системе открытого образования, которые, в свою очередь, определяются на основе знаний, умений и навыков, включающих в себя личностные и профессиональные результаты. Таким образом, каждый уровень описывается в терминах результатов, которые можно сопоставить с существующей системой квалификаций.

В системе открытого образования это включает отбор материалов, поиск информации в библиотеках по ключевым понятиям цифровой экономики, выбор иллюстрирующих примеров интересных фактов и аналогий. Естественный человеческий язык отражает глобальные изменения, происходящие в современном обществе. Многие современные понятия требуют систематического описания, адекватного и эквивалентного перевода, снабжения информационно-аналитическим комментарием с тем, чтобы в полной мере и своевременно отразить направления технологического развития. Цифровая трансформация приводит к тому, что язык трансформируется, и это необходимо своевременно отражать в данном случае к готовящемуся к изданию специализированном «Словаре-справочнике по цифровой трансформации» [1]. Каждую словарную статью словаря-справочника следует рассматривать с точки зрения ее соответствия формируемым компетенциям.

Литература

1. *Макаревич, И.И.* Процесс обучения в условиях цифровой трансформации: необходимость разработки словаря-справочника информационно-коммуникационных технологий цифровой экономики в управленческой деятельности / И. И. Макаревич // Межкультурная коммуникация и профессионально ориентированное обучение иностранным языкам, посвящ. 97-летию образования Белорус. гос. ун-та : материалы XII Междунар. науч. конф., Минск, 26 окт. 2018 г. / Белорус. гос. ун-т, фак. междунар. от-ний ; редкол. : В. Г. Шадурский (пред.) [и др.]. – Минск, 2018. [Электронный ресурс]. – С. 236 – 238. Режим доступа: http://elib.bsu.by/handle/123456789/216183. – Дата доступа: 28.03.2019.

СИСТЕМА ЗАЩИТЫ ИСПОЛНЯЕМЫХ ФАЙЛОВ ЯЗЫКА ПРОГРАММИРОВАНИЯ JAVA

В.А. МАКАРЫЧЕВА

НАУЧНЫЙ РУКОВОДИТЕЛЬ – А.Ф. ОСЬКИН, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК, ДОЦЕНТ

Рассматриваются вопросы защиты программного обеспечения путем применения шифрования скомпилированных файлов языка программирования Java

Ключевые слова: защита программного обеспечения

В настоящее время большинство атак происходит на уровне приложений. Поэтому защита программного обеспечения имеет наивысший приоритет.

Одним из наиболее эффективных методов защиты программного обеспечения является шифрование файлов с исполняемым кодом. Шифрование исполняемых файлов позволяет обеспечить безопасность программного продукта, предотвратить большинство проблем, таких как несанкционированный доступ, внедрение закладок, деятельность сетевых червей и вирусов, использование и модификация программного продукта.

В данной работе применяется шифрование скомпилированных файлов языка программирования Java. Такие файлы имеют расширение .class и содержат байт-код, который выполняет виртуальная машина Java (JVM) в процессе работы программы.

Основная идея разработки состоит в том, что файлы .class будут хранится в зашифрованном виде, а расшифровываться будут в момент загрузки их в JVM. Файлы можно зашифровать любой программой после компиляции, а расшифровывать файлы будет javaagent – программа, способная перехватывать байт-код другой программы при загрузке его в JVM [1].

Одной из основных задач, требующих решения на этапе проектирования является выбор надежного алгоритма шифрования. В качестве такого алгоритма был выбран RC5 (Ron’s Code 5 или

Rivest's Cipher 5) – это блочный шифр, разработанный Роном Ривестом из компании RSA Security Inc. в середине 90-х годов, с переменным количеством раундов, длиной блока и длиной ключа [2].

Расшифровывающая программа разделена на две подсистемы: расшифрования и загрузки байт-кода. В подсистему расшифрования входит класс RC5, который реализует расшифрование массива байт. Данный класс предоставляет функцию расшифрования, в параметрах которой передаются массив зашифрованных байт данных, массив байт ключа, и исходный размер файла .class до шифрования. Функция расшифрования возвращает массив расшифрованных байт данных первоначального размера, т.е. после расшифровки массив уменьшается до размера незашифрованного файла .class.

Ранее говорилось об автоматизации шифрования исполняемых файлов. Эту проблему можно решить с помощью Maven-плагина, который после компиляции зашифрует .class-файлы. Apache Maven – популярный инструмент для сборки Java проектов [3]. Он имеет множество разнообразных плагинов, которые можно использовать во время различных фаз сборки. К тому же есть возможность разработать собственный плагин, об этом и пойдёт речь далее.

Шифрующая программа (Maven-плагин) разделена на три подсистемы: шифрования, взаимодействия с Apache Maven, выработки ключей. Основной функционал подсистемы шифрования и подсистемы выработки ключей реализован в трёх классах: RC5, Encryptor, EncryptionInfoSaver.

Результаты данного исследования могут быть использованы разработчиками и пользователями программного обеспечения для предотвращение несанкционированных воздействий на программный продукт.

Литература

1. Java Agent Development Framework [Электрон. ресурс] / – Режим доступа: http://jade.tilab.com/.
2. Wikipedia RC5 [Электрон. ресурс] / – Режим доступа: https://en.wikipedia.org/wiki/RC5.
3. Apache Maven Project [Электрон. ресурс] / – Режим доступа: http://maven.apache.org/.

ПОДХОД К КОМПЛЕКСНОМУ МЕЖГРУППОВОМУ ТЕСТИРОВАНИЮ ЭРГОНОМИКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А.А. МАРКИНА

НАУЧНЫЙ РУКОВОДИТЕЛЬ – Д.А. КОСТЮК, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК, ДОЦЕНТ

В работе представлена методика и реализующая ее программно-аппаратная система, позволяющие выполнять в ходе эргономической экспертизы программного продукта комплексный учет психофизических параметров пользователя, работающего за персональным компьютером. Рассмотрены оценки нагрузки, воздействующей на пользователя, использование устройств биометрического мониторинга и стандартизированные методы психодиагностики

Ключевые слова: эргономика, межгрупповое тестирование, окулография, психометрия

Подходы, используемые в настоящее время для оценки эргономики графических интерфейсов (как основанные на построении и анализе когнитивных схем, так и использующие специальные приборы отслеживания направления взгляда и/или энцефалографы) имеют существенный недостаток: они не учитывают мотивационную сферу человека, а также особенности его изначального психологического состояния, не вполне выявляют субъективную реакцию пользователя. В настоящей работе предлагается решение данной проблемы сочетанием существующих методик юзабилити-тестирования с методами психодиагностики, касающимися проведения анкетирования и ретроспективы. В свою очередь это позволит повысить точность оценки эргономики программного продукта [1].

Разработка предполагает совместное использование психометрии и биометрических данных (окулографии), поставляемых современными потребительскими устройствами. Для учета психологических особенностей пользователей с последующей классификацией по выделенным типовым паттернам поведения, существенным для интерпретации результатов, предусматривается предварительное прохождение подопытными теста на темперамент (личностный опросник Айзенка), и теста на интеллектуальное развитие (прогрессивные матрицы Равена). Также используются стандартизированные опросники для юзабилити-исследований, применимые в рамках представляемого комплексного подхода: шкала юзабилити системы (SUS), опросник по юзабилити системы после обучения (PSSUQ), а также разработанный Microsoft «инструментарий оценки привлекательности» (англ. Desirability Toolkit). Данная система опросников позволяет собрать комплекс самосообщаемых параметров респондентов (уровень ожидания и удовлетворенности) для их последующего учета при оценке эффективности человеко-машинного взаимодействия [2].

В дополнение к результатам опросов предусматривается контроль темпа работы и корректности выполнения заданий, а также выполняемые в режиме мониторинга биометрические измерения харак-