

1. Гродно. Энцикл. справ. / Белорус. Сов. Энцикл. ; редкол.: И. П. Шамякин (гл. ред.) и др. – Минск : БелСЭ, 1989. – 438 с., [12] л. ил. : ил.

2. *Красовская, В.* Западноевропейский балетный театр. Очерки истории: эпоха Новерра / В. М. Красовская. – Л. : Искусство, 1981. – 286 с., 32 л. ил.

3. Обновленный театр кукол 16 декабря распахнет двери перед зрителем // Гродзенская праўда [Электронный ресурс]. – 2010 – 2015. – Режим доступа : http://region.grodno.by/ru/news/region_news/obnovlennyj-teatr-kukol-16--dekabrja-rasпахnet-dveri-pered-zriteljami_i_12613.html. – Дата доступа : 29.11.2012.

4. Театральная Беларусь : Энциклапедыя : у 2 т. / рэдкал.: Г. П. Пашкоў [і інш.]. – Мінск : БелЭн, 2003. – Т. 2 : Лабанок – Яшчур. – 576 с. : іл.

Б. В. Петренко,
*кандидат технических наук,
доцент кафедры информационных ресурсов;*
И. В. Шкирёнок,
*старший преподаватель кафедры
информационных ресурсов*

ТЕСТИРОВАНИЕ КОМПЬЮТЕРНЫХ ПРОГРАММ И ОБОРУДОВАНИЯ КАК МЕТОД ОБУЧЕНИЯ ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Определяя информационную безопасность как многоуровневую защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые наносят ущерб пользователям и владельцам информации и инфраструктуры, выделим особый аспект проблемы – обучение основам информационной безопасности. Изучение основных понятий в этой области знаний, умения определять угрозы информационным ресурсам и противодействовать атакам на информационные системы не должны осуществляться на самостоятельном (а то и на дилетантском) уровне.

Защита информации – это целый комплекс специальных мероприятий, обеспечивающих информационную безопасность, т. е. поддержание целостности, доступности, когда нужно – конфиденциальности информационных ресурсов, умелое использование приемов ввода, хранения, обработки и передачи

данных. Конечно же, требуются и определенные методы обучения персонала, работающего с информационными ресурсами. Выработать умения и навыки по защите информации возможно в ходе тренинга в учебном процессе, используя для этого прием тестирования компьютерных программ и оборудования.

Есть ряд других эффективных методов обучения основам информационной безопасности. Подтверждение этому – ряд авторитетнейших изданий в поддержку специальных учебных дисциплин в учреждениях высшего и среднего специального образования. Не претендуя на аналитический обзор, укажем только библиографические сведения некоторых новейших академических изданий авторов А. Гринберга, Н. Горбачева, А. Теплякова, В. Ганжи, В. Сидорика, О. Чичко, Васильковых, В. Шаньгина и др. [1; 2; 3; 4; 8]. Лекционные курсы по таким учебным дисциплинам преподают несколько семестров. Многие из этих дисциплин и специальностей не имеют прямого отношения к библиотекам и другим учреждениям информационно-образовательной направленности или культурно-досуговой сферы. Однако система данных знаний в полной мере может влиять на развитие специального образования в области автоматизации библиотечно-информационной деятельности, и в частности – при обучении студентов по дисциплинам «автоматизированные библиотечно-информационные системы», «библиотечные компьютерные сети» и «программно-техническое обеспечение». Их преподавание традиционно осуществляется с дифференциацией: первая из них – для всего потока, две остальные – для группы студентов по специализации «автоматизация библиотечно-информационной деятельности».

Представляя общую концепцию обеспечения информационной безопасности через обучение пользователей тестированию компьютерных программ и оборудования, считаем очень важным дополнить учебно-методические комплексы (учебные программы, пособия, методические разработки) дидактическим материалом об использовании компьютерных антивирусов, программ-чистильщиков, специализированных тестов и сервисного обслуживания операционной системы Windows.

Также, изучая конкретные технологии защиты информационных ресурсов (а это целые параграфы о межсистемных, системных, групповых и персональных технологиях, об управлении рисками и страховании информационных ресурсов), обра-

тим особое внимание на аппаратно-технический аспект безопасности [4; 7; 8]. Общепринятой аксиомой является прямая зависимость информационной безопасности ресурсов и автоматизированных систем от эффективной работы антивирусного программно-технического комплекса. Этот необходимый объем компьютерной грамотности современные пользователи корпоративной сети БГУКИ чаще всего получают от системных администраторов в виде разовых общегрупповых консультаций и индивидуального инструктирования.

Рассматривая, в нашем случае, пользовательский уровень компьютерной подготовленности (т. е. среднестатистического сотрудника, таких же посетителей библиотечных и культурно-досуговых учреждений, а также нынешних студентов факультета информационно-документных коммуникаций), отметим отсутствие у них специальных знаний о работе сетевой версии лицензионного серверного антивируса, необходимой и достаточной конфигурации конкретных сетей персональных компьютеров (ПК), сервисном обслуживании их жестких дисков и в том числе – системного диска (С:).

Подробнее остановимся на знании о специализированных программах-чистильщиках, умении их использовать, что является обязательным минимумом в «санации» ПК. Ведь с течением времени на жестком диске компьютера скапливается много мусора: временные и давно не используемые файлы, их дубликаты, не до конца удаленные программы, различные «логи» и системные данные, ошибки в реестре, отсутствующие записи и многое другое. Все это не только занимает лишнее место, а еще и снижает производительность компьютера. Для очистки операционной системы и жесткого диска от всего этого хлама можно в свободном доступе в Интернете скачать специальные программы-чистильщики, такие, например, как FreeSpacer и CCleaner. Каждая из них – мощнейший бесплатный инструмент, предназначенный для очистки компьютера от различного мусора и ускорения работы операционной системы. Программы имеют понятный русскоязычный интерфейс и благодаря многообразию возможностей призваны оптимизировать ПК, не нарушив при этом стабильности его работы. Наш опыт продолжительного использования программы FreeSpacer явно подтверждает полезность и эффективность очистки компьютеров как на кафедре информационных ресурсов БГУКИ, так и в домашних условиях.

В этой связи, отметим, что в корпоративной локальной сети БГУКИ традиционно используется Антивирус Касперского для Windows Workstations (версия 6.0.4.1424 a.d.f). Но, к сожалению, имеет место такой негативный факт – во второй половине 2015 г. (по завершении предыдущей лицензии) на многих учебных ПК в большинстве компьютерных лабораторий не производится обновление антивирусных баз. Возможно, это недоработка службы системных администраторов в соответствующем подразделении. Мы же настаиваем на необходимости обучить каждого пользователя ПК не только отслеживать работу любой антивирусной программы, но и устанавливать ее, скачивая или покупая лицензионный диск, обновлять или удалять, заменяя на другую.

Это является своего рода апробацией/тестированием как самих программ, так и специальных умений по обслуживанию антивирусного программного обеспечения. Поэтому следует отметить необходимость скорейшего дополнения учебных программ таких дисциплин, как «АБИС» и «программное обеспечение», специальными темами об информационной безопасности и антивирусном обеспечении.

Теперь немного остановимся на тестировании, которое является обязательной частью процесса наладки компьютеров, высокотехнологичных гаджетов (HI-TECH & IT) и производства программного обеспечения (ПО или SOFTWARE). Необходимость тестирования любого из названных рабочих продуктов определяется условиями разработки, продвижения к пользователю и потребителю, факторами его успешной эксплуатации/обслуживания.

Тестирование программного обеспечения и оборудования (testing) – это процесс анализа и/или эксплуатации программного обеспечения с целью выявления и устранения в нем, а также в сопутствующей документации дефектов/ошибок (defect, bug). При этом важно выявление дефектов в тестируемом объекте до того, как эти дефекты будут обнаружены заказчиком или конечным пользователем. Однако полностью протестировать даже несложную программу или оборудование невозможно. Обычная практика тестирования такова: программное средство или тестируемый объект считается пригодным к выпуску, если в нем устранены все обнаруженные критические ошибки и 85 % не критических.

С технологической точки зрения тестирование заключается в выполнении пробных запусков, осуществлении основных функций прибора или программного приложения на некоторых исходных данных и сверке получаемых результатов с заранее известными (эталонными) с целью установить соответствие различных его свойств и характеристик заданным требованиям. Фирмы-производители и коммерческие компании как в нашей стране, так и во всем мире вкладывают все больше средств в процесс тестирования ПО и IT-оборудования. Именно поэтому учебное тестирование как дидактический метод получения и закрепления знаний, умений и навыков обеспечит высокий профессионализм в работе наших выпускников с АБИС (конечно же, при соответствующем уровне преподавания). Подтверждением этому является и работа многих консалтинговых (т. е. консультационных) организаций [5]. Более того, само тестирование выходит на уровень высокотехнологичной автоматизации и получает повсеместное распространение как широко признанные и высоко оплачиваемые компетенции [5, с. 10–12, 268].

Известно, что наибольший эффект в снижении трудоемкости в сфере «НИ-ТЕСН & IT» может быть получен прежде всего на этапах разработки дизайна программного приложения, прибора и их тестирования. Один из путей снижения трудоемкости таких процессов – это их автоматизация. Успешная автоматизация тестирования ПО и приборов дает следующие преимущества:

- сокращение времени исполнения тестов;
- надежность, поскольку устраняется человеческий фактор и сокращает вероятность ошибок;
- скорость и объем выполняемых работ (например, человек никогда не сможет вручную добавить в базу данных (БД) 100 миллиардов записей, составленных из 500 полей каждая);
- сбор статистических данных о работе прибора/приложения и представление ее в удобной для восприятия человеком форме;
- средства автоматизации тестирования в сложных ситуациях способны выполнять «низкоуровневые действия», сложные и/или нежелательные для человека.

Тестирование ПО и оборудования можно классифицировать по самым разнообразным признакам:

- по степени исполнения тестируемого ПО;

- по знанию системы;
- по объекту тестирования;
- по степени изолированности компонентов;
- по признаку позитивности сценариев;
- по времени проведения тестирования;
- по степени подготовленности к тестированию;
- по уровню тестирования;
- по степени автоматизации.

По степени тестируемого ПО выделяют:

- статическое тестирование (static testing);
- динамическое тестирование (dynamic testing).

Статическое тестирование – это процесс анализа самой разработки программного обеспечения, т. е. тестирование без запуска программы. Статическое тестирование предусматривает проверку программного кода, требований к программному продукту, функциональной спецификации, архитектуры, дизайна и т. д.

Динамическое тестирование – это тестовая деятельность, предусматривающая эксплуатацию (запуск) программного продукта. Динамическое тестирование предполагает запуск программы, проверку выполнения ее функциональных модулей и сравнение фактического ее поведения с ожидаемым.

По знанию системы выделяют:

- тестирование «черного ящика» (black box testing);
- тестирование «белого ящика» (white box testing);
- тестирование «серого ящика» (grey box testing).

Более подробно эти вопросы освещаются в монографиях, учебниках и солидных периодических изданиях [6; 7; 8].

1. *Васильков, А. В.* Информационные системы и их безопасность : учеб. пособие / А. В. Васильков, А. А. Васильков, И. А. Васильков. – М. : ФОРУМ, 2014. – 528 с. : ил. – (Профессиональное образование).

2. *Ганжа, В. А.* Компьютерные сети. Информационная безопасность и сохранение информации : учеб.-метод. пособие / В. А. Ганжа, В. В. Сидорик, О. И. Чичко. – Минск : БГУИР, 2014. – 128 с. : ил.

3. *Гринберг, А. С.* Защита информационных ресурсов государственного управления : учебное пособие для вузов / А. С. Гринберг, Н. Н. Горбачев, А. А. Тепляков. – М. : ЮНИТИ-ДАНА, 2003. – 327 с. – (Профессиональный учебник).

4. Информационная безопасность и защита информации : учеб. пособие / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова, Н. Г. Шахов. – Старый Оскол : ТНТ, 2010. – 384 с.

5. Куликов, С. С. Тестирование программного обеспечения. Базовый курс: практ. пособие / С. С. Куликов. – Минск: Четыре четверти, 2015. – 294 с.

6. Тампре, Л. Введение в тестирование программного обеспечения = Introducing Software Testing / Луиза Темпре; [пер. с англ. и ред. А. В. Слепцов]. – М.: Вильямс, 2003. – 368 с.: ил.

7. Чипига, А. Ф. Информационная безопасность автоматизированных систем: учеб. пособие / А. Ф. Чипига. – М.: Гелиос АРВ, 2010. – 336 с.: ил.

8. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М.: ФОРУМ: ИНФРА-М, 2014. – 416 с.: ил. – (Профессиональное образование).

*А. М. Пісарэнка,
кандыдат філалагічных навук,
загадчык кафедры беларускай філалогіі
і сусветнай літаратуры*

ЛІТАРАТУРНАЯ ТВОРЧАСЦЬ ЯК СПАСАБ САМАРЭАЛІЗАЦЫІ АСОБЫ: АНАЛІЗ ДЗЕЙНАСЦІ АБ'ЯДНАННЯ «БУКЕТ»

Літаратурна-творчае аб'яднанне «БУКет» было створана пры кафедры беларускай філалогіі і сусветнай літаратуры БДУКМ у кастрычніку 2001 года. Яго арганізатары – А. М. Пісарэнка (паэт, член СПБ Алена Багамолава) і старшы выкладчык Н. В. Дзянісава (літаратурны крытык, член СБП Наталля Якавенка). З 2004-га да працы актыўна далучылася старшы выкладчык В. В. Шунейка, апошнім часам літкансультантам аб'яднання сталі таксама прафесар В. С. Варапаева, старшы выкладчык Л. І. Даніленка. Восенню 2008 года аб'яднанне было пераведзена на студэнцкае самакіраванне. Новым кіраўніком стаў студэнт ФІДК (цяпер супрацоўнік аддзела менеджменту якасці) Павел Макееў, а ўвосень 2015-га кіраўніком аб'яднання быў абраны студэнт ФТБКіСМ Уладзімір Сергіенка.

Вынікам працы аб'яднання сталі 10 зборнікаў вершаў і прозы: «БУКет», «Акварэлі», «Завіруха кропель», «Каліва», «Кветка ў мегаполісе», «Дар зямны», «Весніцы», «Світальныя словы», «Ляці Вышэй!», «Вітаю цябе, Натхненне!». Апрача таго, творы «букетаўцаў» неаднаразова друкаваліся і друкуюцца ў рэспубліканскіх газетах «Літаратура і мастацтва», «Наша слова», часопісах «Маладосць», «Літаратурны квартал», «Альфа-