УДК 37.046.4 004.5

Филяк П.Ю., Фадеев А.Н.
Сыктывкарский государственный университет имени Питирима Сорокина
E-mail: paralax-1@yandex.ru ; accroach@gmail.com

ИНТЕРНЕТ-ТРЕНАЖЕР ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Статья посвящена вопросам разработки и внедрения интегрированной обучающе-контролирующей системы с использованием, в том числе, интернет-ресуров и обучающее-контролирующих сред, представляющих глобальные и локальные информационные ресурсы, для обеспечения информационной безопасности организации в целях предотвращения и защиты от угроз со стороны сотрудников организации, не обладающих требуемым уровнем компетентности или ответственности, а также со стороны внешних нарушителей.

Наиболее актуальным на современном этапе является создание интегрированной обучающе-контролирующей среды (системы) для обеспечения информационной безопасности. Для организации, которая заботится о длительных перспективах развития, важным является обучение и контроль знаний своих сотрудников. Поэтому, по отношению к ним, требуются серьезные теоретические и практические знания в сфере их деятельности.

Требования к уровню знаний специалистов, с одной стороны, устанавливаются нормативными правовыми, с другой – могут определяться внутренними корпоративными стандартами организации. Реальность такова, что законодательство постоянно изменяется – так в последнее время в сфере информационной безопасности принято много новых нормативных правовых актов. Кроме того, технологии не стоят на месте, перед работодателями встает потребность в качественном подборе персонала, отвечающего всем требованиям. Все это приводит к необходимости создания современной системы обучения и проверки знаний. Такая реально действующая система и была разработана авторами статьи, что и описывается ниже в представленной публикации.

Ключевые слова: обучающее-контролирующая среда, обеспечение информационной безопасности, тестирование, периодический контроль, мониторинг, глобальные и локальные информационные ресурсы, интернет-ресурсы.

Проверка и периодический контроль знаний специалистов необходимы по причине развития процессов информатизации общества, которые особенно ярко наблюдаются в последние десятилетия [1]–[5]. Наиболее актуальным на современном этапе является создание интегрированной обучающе – контролирующей среды (системы) для обеспечения информационной безопасности [6]–[8]. Требования к уровню знаний специалистов, с одной стороны, устанавливаются нормативными правовыми актами Российской Федерации [9]–[11], с другой – могут определяться внутренними корпоративными стандартами организации. Для организации, которая заботится о длительных перспективах развития, важным является непрерывное обучение и контроль знаний своих сотрудников в целях предотвращения и защиты от угроз со стороны некомпетентных и безответственных работников и посягательств извне. Для этого необходима информационная система (тренажер), позволяющая эффективно осуществлять обучение и тестирование персонала организации.

Идея создания обучающе-тестирующего тренажера – программно-аппаратного комплекса (ПАК) путем разработки специальных информационных систем (ИС) или на базе использования уже существующих ИС, с набором соответствующих располагаемых прикладных инструментальных средств, не нова и по сути и достаточно тривиальна, если не заложить в ее разработку определенных требований и параметров, задающих новизну и существенные отличия, а в идеале – уникальность. В этой связи, до разработки такой системы (среды) прежде всего следует провести тщательный анализ целей и задач, которые преследует разработчик – сформулировать, так называемые, ЭТТ – эксплуатационно-технические требования к создаваемому тренажеру:

- системность и непрерывность обучения;
- поддержание знаний сотрудников на соответствующем уровне и повышение их профессиональной квалификации – быстрое реагирование на внешние и внутренние изменения, в том числе к изменениям в законодательстве;
- возможность привлечения и использования всех открытых источников, современных актуальных баз знаний, данных и документов как российских, так и международных;
- эффективность, апробированность и сертифицированность используемых инструментальных средств их современность и соответствие требованиям времени;

• юридическая правомерность использования применяемых инструментальных средств, компонентов и системы в целом;

• надежность и простота;

• возможность обеспечения индивидуализации процессов обучения и контроля;

• удобство программного обеспечения и интерфейса, создающие условия для мотивации обучения и тестирования, обеспечение отсутствия (или минимизации) рутинных процедур;

• обеспечение объективности тестирования;

• возможность сбора, обработки, хранения и накопления информации, связанной с проведением обучения и тестирования;

• возможность обезличивания результатов обучения и тестирования;

• обеспечение возможности работы с информацией ограниченного доступа с соблюдением требований информационной безопасности;

• высокая степень автоматизированности систем обучения и проверки знаний;

• возможность обеспечения непрерывного мониторинга, контроля и координации текущих процессов обучения и получаемых результатов;

• возможности дифференциации обучения и тестирования по различным критериям;

• прочие требования

В базовом подходе предполагается разделение тестирования и обучения на две группы:

1. Для сотрудников организации, использующих автоматизированное рабочее место в качестве инструмента исполнения профессиональных обязанностей.

2. Для специалистов, обеспечивающих информационную безопасность.

Для сотрудников, не связанных с обеспечением информационной безопасности, достаточно контроля базовых знаний: знание продуктов Microsoft Windows, Microsoft Office, общее понятие о файлах и папках, навыки работы в локальной и сети интернет, умение распечатать документ на локальный или сетевой принтер и т.д.

Для специалистов, обеспечивающих информационную безопасность, обучение в области информационной безопасности, к сожалению, часто является по сути формальным и декларативным, так как традиционно подразумевает под собой обязательное изучение нормативных правовых актов и внутренних стандартов, локальных нормативных актов и т.д. по устоявшимся методикам «прочитал – выучил – (за невостребованностью изученного) забыл».

Традиционный подход к обучению обязательно должен заканчиваться проверкой знаний. Поэтому структура учебного курса должна выглядеть следующим образом:

• учебные материалы (это могут быть как официальные нормативные документы, так и учебные пособия, разработанные на их основе);

• контрольные задания (при электронном обучении контрольные задания, как правило, представлены в виде тестовых вопросов).

Обучаясь по данной системе, работники смогут получить именно те знания, которые им необходимы для эффективности их профессиональной деятельности. В дальнейшем, если система была создана на основе нормативных правовых актов, то по мере их изменения, отмены или ввода новых документов должна осуществляться актуализация учебного курса, как учебных материалов, так и контрольных заданий.

При разработке автоматизированной системы обучения и контроля знаний в области информационных и коммуникационных технологии (ИКТ) и информационных систем (ИС) необходимо помнить о реализации основных методологических принципов, среди которых (рис. 1):

• полнота (курс должен обязательно разбиваться на отдельные темы, их совокупность обеспечивает рассмотрение всех требуемых вопросов);

• достоверность (все нормативные материалы аутентично воспроизводятся в электронном виде в соответствии с официальным опубликованием документов);

• своевременность (получение актуальных знаний);

• целостность (ни одно из заданий (вопросов) не может быть изъято из системы без потери ее качественных показателей);

• универсальность (тестовые задания могут использоваться при закреплении знаний, полученных при изучении отдельных тем, и на основе этих же тестовых заданий могут быть составлены контрольные задания) [12].

Методологию подхода к обучению и тестированию можно наглядно представить с помощью следующей блок-схемы (рис. 2).

Платформами для разработки интегрированной обучающее-контролирующей системы для обеспечения информационной безопасности организации могут выступать Microsoft Office и Microsoft SharePoint Workspace 2010. Возможности данных приложений позволяют осуществить такие функции как:

• Тестирование. С помощью встроенного приложения Microsoft Excel имеется возможность создания тестов и отображения результата с последующим занесением в базу данных.

• Ведение отчетов. Благодаря приложению Microsoft Access есть возможность формировать отчеты, исходя из итогов тестирования.

• Планирование. Microsoft Outlook служит напоминанием сотрудникам организации о необходимости повторного прохождения тестирования с целью подтверждения своей профессиональной пригодности.

• Хранение. Microsoft Word необходим для накопления и сохранения нормативных правовых актов (Рис.3), предсталенных в формате данного редактора.

Одной из особенностей данной системы является автономность. Пользователь получает возможность использовать систему без платформы Microsoft SharePoint Workspace 2010. Тесты, составленные в программном продукте Microsoft Office, отправляются лично экзаменуемому при помощи электронной почты или корпоративной сети. После прохождения тестирования отсылаются обратно. Далее при помощи языка программирования Visual Basic for Application данные переносятся в таблицу, в программный продукт Microsoft Access, где и накапливается вся основная статистика. По итогам сотрудники прошедшие тестирование могут приступать к своим функциональным обязанностям, те специалисты, что показали неудовлетворительный результат, отправляются на повторное обучение.

Другой характерной особенностью системы является возможность обезличивания обучающихся и тестируемым, что является очень важным условием обеспечения информационной безопасности организации.

Еще одной, очень важной, функцией разработанной системы можно назвать возможность корректировки моделей нарушителей организации – на основании результатов тестирования сотрудников и обучающихся, с помощью данной системы.

В качестве обучающей составляющей выступают две самые распространенные среды дистанционного обучения: Moodle и eFront [13]–[14]. С помощью среды дистанционного обучения можно: автоматизировать и ускорить процессы обучения и оценки, эффективно распределить нагрузку, снизить затраты на органи-

Рисунок 1. Автоматизированная система обучения и контроля знаний

зацию учебного процесса, и повысить эффективность обучения в целом [15].

Moodle (модульная объектно-ориентированная динамическая учебная среда) – это свободная система управления обучением, ориентированная, прежде всего на организацию взаимодействия между контролирующим и обучающимися, хотя подходит и для организации традиционных дистанционных курсов, а также поддержания очного обучения [15].

eFront – представляет собой новое поколение eLearning систем, сочетающее в себе функции систем управления обучением (LMS – Learning Management System) [13].

Возможности eFront позволяют решать задачи организации учебного процесса, а также задачи повышения квалификации, аттестации и отбора сотрудников в организациях различного масштаба. Применение системы позволяет решать задачи образования эффективнее, легче и проще. Основу системы представляет eFront Core – система, распространяемая со свободной лицензией, реализующая основные функции LMS/LCMS [13]. Схема взаимодействия компонентов системы представлена на рисунке 4.

Таким образом, можно сделать выводы, что создание автоматизированной системы обучения и проверки знаний позволяет обеспечить:

• снижение потерь от неправильной оценки ситуации и неправильных действий работников, в связи с закреплением техническими системами, в процессе, обучения навыков более грамотного управления;

• предотвращение ущерба от непредвиденного наступления нежелательных событий и ситуаций – ограничение распространения так

Рисунок 2. Методология подхода к обучению и тестированию

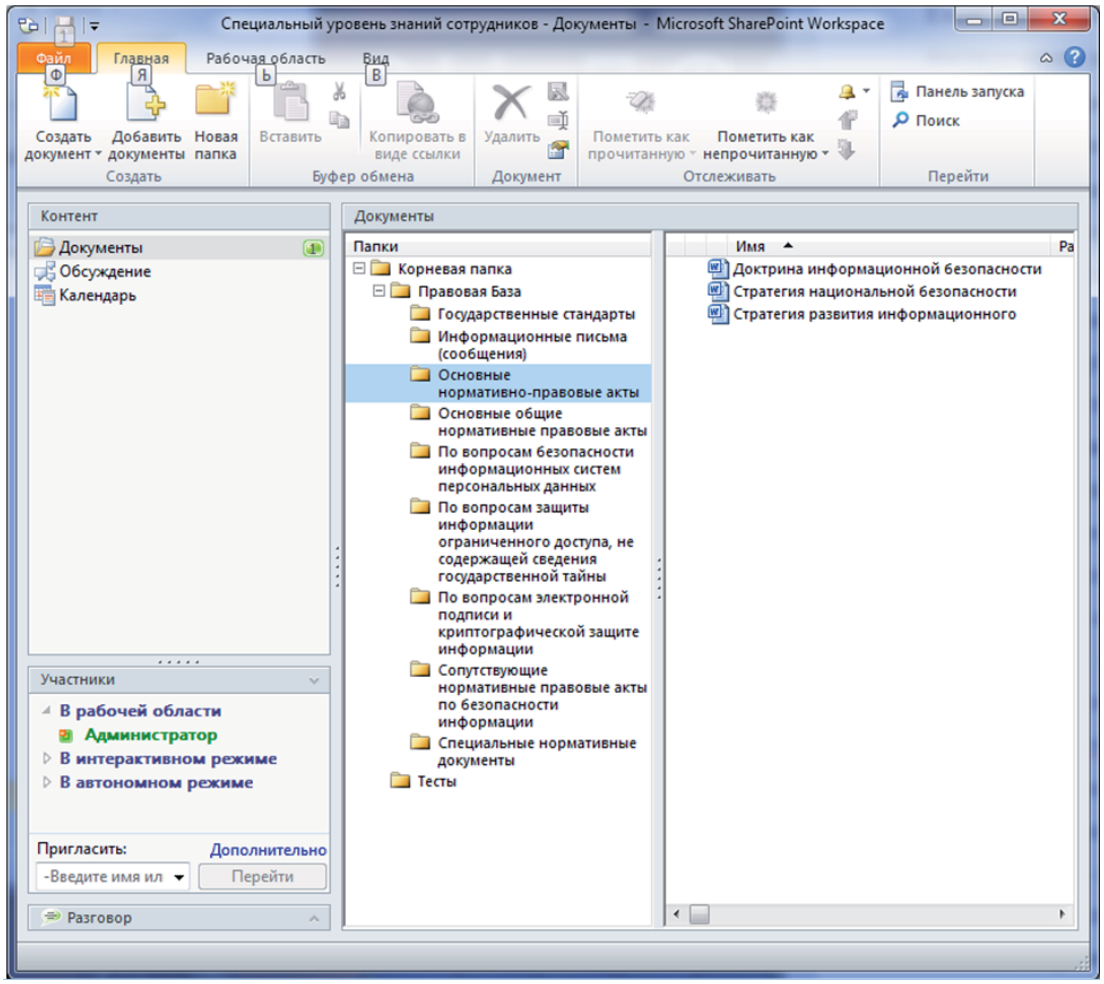

Рисунок 3. Хранение и накопление информации

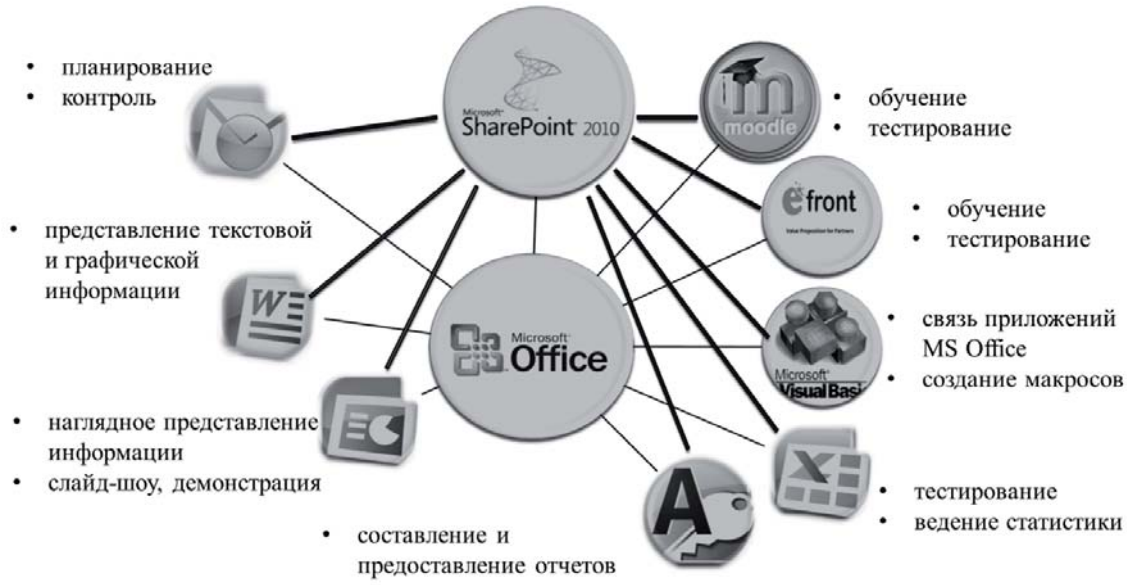

Рисунок 4. Схема работы интегрированной обучающе – контролирующей системы для обеспечения информационной безопасности организации

называемых «цепочек нежелательного развития событий» («эффект домино»);

• снижение вероятности аварий и поломок оборудования, угроз жизни и здоровью людей;

• укрепление корпоративного сознания работников, сближение личных интересов работников с интересами компании;

• рост способности к координированной осознанной совместной деятельности и принятию решений;

• обмен информацией между работниками различных предприятий, проходящими обучение вместе, распространение «по горизонтали» передового опыта, других инноваций.

10.08.2015

Список литературы:

1. Филяк П.Ю. Информационная и экономическая безопасность в условиях информационного общества. Вестник ИТАРК № 1, 2011. с. 51 – 53.
2. Филяк П.Ю. Актуальность обеспечения обеспечения информационной и экономической безопасности в условиях информационного общества. Известия Тул ГУ. Технические науки. Вып. 3. Тула: Изд-во ТулГУ, 2013. с. 262-267.
3. Филяк П.Ю. Обеспечение информационной и экономической Безопасности в условиях глобальной информатизации. Сборник трудов VI Международной научно-практической конференции студентов, аспирантов и молодых ученых. – М.: Изд-во Финансового университета, 2013. с. 20– 27.
4. Филяк П.Ю. Информационная и экономическая безопасность в условиях глобальной информатизации. Современные проблемы безопасности жизнедеятельности: настоящее и будущее: Материалы III Международной научно-практической конференции в рамках форума «Безопасность и связь». Часть I. – Казань: ГБУ «Научный центр безопасности жизнедеятельности», 2014. – с. 444-448.
5. Филяк П.Ю. Проектирование с учетом обеспечения безопасности. Журнал. «Информация и безопасность», Т. 18. № 1. Воронеж, ВГТУ, 2015.– с. 101 – 106.
6. Филяк П.Ю. Компетентностный подход к обучению информационным технологиям. Вестник ИТАРК № 2, 2011. с. 42–48.
7. Филяк П.Ю., Власов В.А., Щанова А.А. Разработка правового навигатора для изучения дисциплины информационная безопасность. Современные проблемы и задачи обеспечения информационной безопасности: труды Всероссийской научно-практической конференции «СИБ-2014». М.,МФЮА, 2014. – с. 225-233.
8. Филяк П.Ю., Комиссарова Г.Н. Создание комплексной системы защиты информации с учетом роли кадров. Современные проблемы и задачи обеспечения информационной безопасности: труды Международной научно-практической конференции «СИБ-2015». М.,МФЮА, 2015. – с. 47-50.
9. Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ
10. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ
11. «Доктрина информационной безопасности Российской Федерации» от 09.09.2000. Пр. № – 1895
12. Н.В. Гришина «Организация комплексной системы защиты информации». М.: «Гелиос АРВ», 2007. 256 с.
13. eFront – свежие технологии обучения! [Электронный ресурс] // URL: http://www.abbris.ru/?p=efront – Электрон. дан. – ООО АББРИС, 2007, (Дата обращения 14.03.2015).
14. Поддержка Office [Электронный ресурс] URL https://support.office.com/ (Дата обращения 21.05.2015).
15. Moodle – система дистанционного обучения [Электронный ресурс] // URL: http://www.opentechnology.ru/products/moodle – Электрон. дан. – М.: ООО «Открытые технологии» (Дата обращения 15.05.2015).

Сведения об авторах:

Филяк Петр Юрьевич, доцент кафедры информационной безопасности
Сыктывкарского государственного университета имени Питирима Сорокина, кандидат технических наук
E-mail: paralax-1@yandex.ru

Фадеев Андрей Николаевич, обучающийся Сыктывкарского государственного университета
имени Питирима Сорокина
E-mail: accroach@gmail.com