МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

«СОЗДАНИЕ ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА В УСЛОВИЯХ РЕАЛИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ»

Магистерская диссертация
по направлению 44.04.04 «Профессиональное обучение»,
программа магистратуры «Управление информационной безопасности в профессиональном образовании»

Выполнила:
магистрант группы ЗФ-309-210-2-1
Гафарова Екатерина Александровна
Научный руководитель:
д.т.н., профессор кафедры
АТ,ИТ и МОТД Дмитриев Михаил Сергеевич

Проверка на объем заимствований:
91,25 % авторского текста

Работа рекомендована к защите
«01» февраля 2019 г.
Зав. кафедрой АТ,ИТиМОТД
_____ В.В. Руднев

Челябинск, 2019

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
Профессионально-педагогический институт
Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Направление подготовки 44.04.04 – Профессиональное обучение (Управление информационной безопасностью в профессиональном образовании)

З А Д А Н И Е

на выпускную квалификационную (магистерскую) работу

1. Студентке Гафаровой Екатерине Александровне, обучающейся в группе ЗФ-309/210-2-1 по направлению подготовки 44.04.04 «Профессиональное обучение («Управление информационной безопасностью в профессиональном образовании»)».

Научный руководитель квалификационной работы: «СОЗДАНИЕ ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА В УСЛОВИЯХ РЕАЛИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ» д.п.н., профессор кафедры профессор кафедры АТ,ИТиМОТД Дмитриев Михаил Сергеевич.

Тема магистерской диссертации: утверждена приказом ректора Южно-Уральского государственного гуманитарно-педагогического университета № 580-сз от «26» апреля 2017 г

2. Срок сдачи магистрантом законченной работы на кафедру 18 февраля 2019 года

3. Содержание и объем работы (пояснительной расчетной и экспериментальной частей, т.е. перечень подлежащих разработке вопросов).

1)Раскрыть специфику электронных образовательных ресурсов, их дидактические возможности, функционал, этапы создания, критерии оценки.

2)Исследовать защищенность электронных образовательных ресурсов на базе исследования – в ГПБОУ «ЮУрГТК»

3)Выявить основные направления политики информационной безопасности ГПБОУ «ЮУрГТК»

4)Разработать электронный образовательный ресурс для образовательной организации СПО - ГПБОУ «ЮУрГТК»

5) Предложить меры и провести их апробацию по обеспечению требований политики информационной безопасности электронных образовательных ресурсов в ГПБОУ «ЮУрГТК».

4. Материалы для выполнения магистерской работы:

1) Учебная, нормативно-правовая, научно-техническая, педагогическая, методическая литература по теме магистерской работы.

2) Материалы преддипломной практики по теме магистерской работы.

5. Перечень графического материала (с точным указанием обязательных таблиц, чертежей или графиков, образцов и др.).

1) Таблицы.

2) Рисунки и диаграммы

6. Консультанты по специальным раздела магистерской работы:

Раздел	Консультант	Отметка о выполнении
Педагогика		
Информационная безопасность		
Экономика		
Охрана труда		

Дата выдачи задания «_»_..... 201..._ года

Задание выдал _____ **Дмитриев М.С.,** профессор, д.п.н.

Подпись научного руководителя Фамилия, Имя, Отчество, ученое звание и степень

Задание принял Гафарова Екатерина Александровна

Подпись студента Фамилия, Имя, Отчество студента

КАЛЕНДАРНЫЙ ПЛАН

№ п/п	Наименование этапов подготовки выпускной квалификационной (магистерской) работы	Срок выполнения этапов ВКР	Отметка о выполнении
1.	Предзащита ВКР		
2.	Доработка ВКР после предзащиты		
3.	Нормоконтроль		
4.	Подписание ВКР научным руководителем		
5.	Оформление пояснительной записки и презентации ВКР		
6.	Подписание рецензии наВКР		
7.	Защита ВКР на заседании ГАК		

Автор ВКР Гафарова Екатерина Александровна _____

Фамилия, Имя, Отчество студента Подпись студента

Научный руководитель ВКР

Дмитриев М.С., профессор, д.п.н.. _____

Фамилия, Имя, Отчество, ученое звание Подпись научного руководителя

Заведующий кафедрой Руднев Валерий Валентинович, доцент, к.т.н._____

Фамилия, Имя, Отчество, ученое звание Подпись заведующего кафедрой

СОЗДАНИЕ ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА В УСЛОВИЯХ РЕАЛИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ.

Введение

Образовательные организации в настоящее время сталкиваются с серьезными проблемами в обеспечении информационной безопасности своих информационных ресурсов. Информационные ресурсы и информационные системы относятся к ряду основных защищаемых элементов во всех сферах жизнедеятельности современных организаций среднего профессионального образования.

Информационная безопасность - это защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести недопустимый ущерб субъектам информационных отношений.

В отечественной и зарубежной литературе в настоящее время немалое внимание уделяется проблемам информационной безопасности.

Проблема исследования информационной политики, развития информационного пространства в Российской Федерации были рассмотрены в работах: М.С. Вершинина, К.В. Ветрова, С.Э. Зуева, В.Д. Попова, А.И. Ракитова. Особый вклад в исследование информационной безопасности в различных сферах общества, культуры, науки и техники, внесли такие ученые и исследователи, как А.Б. Агапов, А.С. Алексеев, И.Л. Бачило, А.В. Возженников, Ю.М. Горский, Г.Н. Горшенков, И.С. Даниленко, Н.В. Данилов, С.А. Дятлов, Г.Г. Феоктистов, А.М. Яновский и другие. В работах этих ученых сформулированы концептуальные положения о сущности и содержании категорий информационной безопасности, исследованы их взаимосвязи, обоснованы приемы и способы исследования и обеспечения информационной безопасности и различных составляющих системного подхода.

Важное значение с точки зрения объекта и предмета настоящего исследования имеют также работы А.В. Кульбы, А.С. Рябцева, К.В. Станиславчика, А.Б. Табакова.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности хранения информации имеет особое значение. К таким информационным системам можно отнести, например, банковские или юридические системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным. Для образовательных организаций существенным становится защита информационных ресурсов.

В настоящее время, несмотря на большое количество работ по проблематике информационной безопасности, следует отметить, что ее теоретическая изученность явно недостаточна, практические методики по формированию оптимального механизма информационной безопасности в образовательных организациях не соответствуют условиям реального времени. В работах отечественных и западных авторов превалирует односторонний подход в исследовании проблем информационной безопасности, рассматривается какая-то одна сторона из всего механизма информационной безопасности в организациях вообще.

Для того чтобы отразить подход к защите информационных активов образовательной организации необходимо разработать политику информационной безопасности, при этом каждая организация должна осознать необходимость поддержания соответствующего режима безопасности и выделения на эти цели значительных ресурсов.

Политика информационной безопасности - свод документов, в которых рассматриваются вопросы организации, стратегии, методов и процедур в отношении конфиденциальности, целостности и доступности информационных ресурсов организации. Политика безопасности строится на основе анализа рисков - процесса определения угроз безопасности системы и отдельным ее компонентам, определение их характеристик и потенциального ущерба.

Конечная цель разработки политики информационной безопасности - обеспечить целостность, доступность и конфиденциальность для каждого информационного ресурса, в частности, электронных образовательных ресурсов, значение которых в современной педагогической практике только возрастает благодаря продолжающейся интенсивной информатизации профессионального образования, так как образовательный процесс требует разработки и внедрения все новых интерактивных форм электронных средств.

Специфика образовательных организаций состоит в отсутствии стандартного подхода при проведении информатизации объектов профессионального образования, в связи с чем, каждая образовательная организация имеет уникальную корпоративную сеть, со своими особенностями, сложившимися пользовательскими традициями, разной степенью обеспеченностью квалифицированными кадрами, различными техническими характеристиками и разнородными архитектурными решениями. Обновление и усовершенствование программно-аппаратного базиса корпоративной сети образовательной организации в связи с постоянно обновляющимися угрозами информационной безопасности должно происходить с учетом специфики такой сети и в соответствии с эффективными трендами обеспечения информационной безопасности, реализуемыми при комплексном подходе.

К наиболее эффективным направлениям относятся технологии виртуализации, в частности, создание так называемых «песочниц». Песочница (англ. sandbox) – специальный механизм для безопасного исполнения программ, используются как часть проактивной защиты от вредоносного кода и сетевых атак является контролируемым набором ресурсов для выполнения гостевой программы.

Потребность в создании оптимальной системы информационной безопасности посредством реализации требований политики информационной безопасности при создании и применении электронных

образовательных ресурсов, а также проработка вопросов использования все более совершенных методов обеспечения информационной безопасности образовательных организаций определили **актуальность** настоящего исследования.

Целью исследования является разработка электронного образовательного ресурса в условиях реализации политики информационной безопасности ГБПОУ «ЮУрГТК».

Объектом исследования выступает образовательный процесс в образовательной организации среднего профессионального образования (СПО) - ГБПОУ «ЮУрГТК», а **предметом исследования** – процесс применения электронного образовательного ресурса в образовательном процессе организации СПО.

Гипотеза исследования состоит в предположении о повышении защищенности информационных ресурсов образовательной организации при реализации комплексного подхода обеспечения безопасности образовательного процесса с применением технологий виртуализации посредством реализации изолированной среды (песочницы) и настройки сетевых правил для ограничения несанкционированного доступа в изолированную среду.

Для достижения поставленной цели в работе решались следующие **задачи:**

1) Изучить научно-методические, технические информационные источники, на основе которых провести анализ содержания, структуры, дидактических возможностей, функционала, места в образовательном процессе современной образовательной организации, этапов разработки и критериев оценки электронных образовательных ресурсов;
2) Провести анализ требований ГОСТ в области создания электронных образовательных ресурсов;

3) Проанализировать состояние защищенности электронных образовательных ресурсов в ГБПОУ «ЮУрГТК», выявить существующие уязвимости.
4) Выявить подходы к совершенствованию информационной защиты электронных образовательных ресурсов в ГБПОУ «ЮУрГТК».
5) Разработать электронный образовательный ресурс для профессионального модуля ГБПОУ «ЮУрГТК»
6) Предложить меры информационной защиты и провести их апробацию на базе ГБПОУ «ЮУрГТК».

Методологическую основу исследования составляют системный подход, метод моделирования, метод сравнения и аналогии, метод динамических испытаний и другие.

Научная новизна проведенных исследований и полученных в работе результатов заключается в следующем:

- показана возможность необходимого обновления существующей системы комплексной безопасности образовательного процесса в образовательной организации среднего профессионального образования путем реализации технологий виртуализации и настройки сетевых правил для ограничения несанкционированного доступа в изолированную среду.

Практическая значимость работы заключается в следующем:

- разработан электронный образовательный ресурс по профессиональному модулю в ГПБОУ «ЮУрГТК», который может быть использован и в других образовательных организациях СПО;
- реализована изолированная виртуальная среда (песочница) для проактивной защиты информационных ресурсов;
- проведена апробация сетевых правил для ограничения несанкционированного доступа в изолированную среду.

Проведенные исследования и полученные результаты могут быть использованы для повышения эффективности комплексной системы защиты информационных ресурсов в образовательных организациях.

Ход исследования и его результаты докладывались и обсуждались на международных конференциях:

1. Международная научно-практическая конференция «ADVANCES IN SCIENCE AND TECHNOLOGY», Москва, 31 июля 2017 года. Публикация: «Концепция обеспечения информационной безопасности в образовательной организации»./[Текст] Азарова Е.А., Гафарова Е.А.//Сб. материалов межд. научн-практ. конференции , Москва, НИЦ «Актуальность РФ», 2017 с. 143-146
2. Международной научно-практической конференции «Непрерывное образование в интересах устойчивого развития: новые вызовы», Казахстан, Қостанай, 6 декабря 2018 года. Публикация: «К вопросу реализации принципов информационной защиты электронных образовательных ресурсов в образовательных организациях». [Текст]/Е.А. Гафарова.// Сборник материалов Международной научно-практической конференции «Непрерывное образование в интересах устойчивого развития: новые вызовы». Национальная академия образования им.И. Алтынсарина. – Астана, 2018 г.– с. 413-416.

База исследования: ГБПОУ СПО «Южно-Уральский государственный технический колледж», г. Челябинск.

Диссертационная работа состоит из введения, трех глав, заключения, библиографического списка и приложений.

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДИЧЕСКИЕ ОСНОВЫ СОЗДАНИЯ ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА ДЛЯ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1. Электронные образовательные ресурсы: дидактические возможности, функционал, место в образовательном процессе современной образовательной организации СПО

Сущность, содержание и общие требования к созданию и использованию электронных образовательных ресурсов (далее – ЭОР) определены в ГОСТ Р 53620-2009 Информационно-коммуникационные технологии в образовании. Электронные образовательные ресурсы. Общие положения [1].

ЭОР является основополагающим компонентом информационно-образовательной среды (далее – ИОС), ориентированным на реализацию образовательного процесса с помощью информационно-коммуникационных технологий и на применение новых методов и форм обучения: электронное обучение, мобильное обучение, сетевое обучение, автономное обучение, смешанное обучение, совместное обучение [18], [21], [27]. Структура, предметное содержание и метаданные ЭОР должны соответствовать их назначению в образовательном процессе и требованиям, обусловленным спецификой функционирования в ИОС.

Все многообразие ЭОР условно можно подразделить на информационные источники и информационные инструменты.

В образовательном процессе возможно использование как простых информационных источников (звук, изображение, текст, видеоматериалы, модели), так и комплексных, содержащие простые информационные источники, связанные с гиперссылками, например, мультимедиа энциклопедии.

Информационный инструмент учебной деятельности – это программный продукт, позволяющий производить активные действия над информационными источниками (объектами), создавать их, менять, связывать, передавать и т.д.

К педагогическим ЭОР также относятся электронные учебные издания и электронные учебные материалы.

ЭОР подразделяются на:

- мультимедийные продукты;
- программные продукты;
- изобразительные продукты;
- аудио продукты;
- текстовые продукты;
- электронные аналоги печатных изданий.

Цели использования ЭОР различны и многообразны:

- повышение эффективности обучения и качества знаний обучающихся;
- развитие познавательной активности;
- повышение интереса к изучаемому предмету;
- развитие аналитического мышления;
- формирование навыков работы с компьютером;
- формирование навыков коллективной работы;
- формирование навыков самостоятельного исследования.

Функциональные возможности применения ЭОР в образовательном процессе в значительной степени определяются их дидактическими свойствами, такими как интерактивность, коммуникативность, возможность представления учебных материалов (текст, графика, анимация, аудио, видео) средствами мультимедиа, применением компьютерного моделирования для исследования образовательных объектов, а также автоматизация различных видов учебных работ [27], [36].

Применение ЭОР в образовательном процессе в сочетании с системами управления обучением и управления образовательным контентом позволяет

эффективно реализовать: организацию самостоятельной когнитивной деятельности учащихся; организацию индивидуальной образовательной поддержки учебной деятельности каждого учащегося преподавателями; организацию групповой учебной деятельности с применением средств информационно-коммуникационных технологий [26], [33].

Функциональная структура ЭОР должны соответствовать их назначению в образовательном процессе и специфике уровней образования и изучаемых дисциплин (предметов).

Типовая структура комплекса ЭОР по дисциплине для обеспечения изучения дисциплин образовательной программы высшего и среднего профессионального образования включает следующие основные системные элементы: а) учебная программа по изучаемой дисциплине ;б) электронный курс лекций; в) электронный учебник; г) лабораторный практикум удаленного доступа; д) учебные пакеты прикладных программ; е) система контроля знаний [35], [36].

Структура ЭОР может быть представлена в виде блоков учебного материала, представляющих собой совместно используемые объекты содержания (фрагменты текста, графические иллюстрации, элементы гипермедиа, программы). Размещение совместно используемых объектов содержания в сетевых депозитариях обеспечивает их многократное применение для создания новых ЭОР методом агрегации [27].

ЭОР могут быть классифицированы по следующим признакам:

а) способу применения в образовательном процессе;

б) целевому уровню и ступени образования;

в) форме обучения;

г) тематике;

д) целевой аудитории;

е) типу ЭОР;

ж) целевому назначению;

з) функции, выполняемой в образовательном процессе;

и) степени дидактического обеспечения специальности;

к) виду образовательной деятельности;

л) характеру представления информации;

м) степени интерактивности;

н)степени соответствия действующим государственным образовательным стандартам.

В свою очередь по способу применения в образовательном процессе ЭОР классифицируются следующим образом: распределенные ЭОР, размещенные в различных ИОС (порталы, электронные библиотеки, хранилища, системы дистанционного обучения) и используемые в режиме удаленного доступа на основе Интернет-технологий; ЭОР для применения в локальных сетях образовательных учреждений и организаций; однопользовательские ЭОР, предназначенные преимущественно для использования на персональных компьютерах (для данной группы характерно использование носителей CD и/или DVD).

Типология ЭОР представлена на рис. 1

Рисунок 1

Рубрикация ЭОР в соответствии с их классификационными признаками применительно к образовательным Интернет-порталам федерального уровня определена ГОСТ Р 52657 Информационно-коммуникационные технологии в образовании. Образовательные интернет-порталы федерального уровня. Рубрикация информационных ресурсов [2].

ЭОР являются продуктом, создаваемым на основе знаний о предметной области с использованием педагогических методов, дидактических подходов и средств информационно-коммуникационных технологий. Комплекс отличительных свойств, определяющих присущие ЭОР характеристики качества, может быть условно разделен на три основные группы.

I. отличительные свойства, характеризующие соответствие структуры и содержания ЭОР требованиям федеральных образовательных стандартов, образовательных программ, нормативных и учебно-методических документов.
II. отличительные свойства, характеризующие ЭОР с точки зрения педагогических, дидактических и психологических аспектов его использования в образовательном процессе.
III. отличительные свойства, характеризующие ЭОР как продукт информационно-коммуникационных технологий с учетом специфики его использования в информационной образовательной системе.

1.2 Этапы и общие принципы создания электронных образовательных ресурсов

Приведем описание этапов создания ЭОР.

ЭОР должны создаваться при наличии потребности в применении их в образовательном процессе, при этом они должны обеспечивать качество подготовки специалистов, соответствовать современному научно-техническому уровню, обеспечивать творческое и активное овладение

обучающимися знаниями, умениями и навыками, предусмотренными целями и задачами учебного процесса, а также отличаться высоким уровнем технического исполнения и художественного оформления, полнотой информации, качеством методических приемов, наглядностью, логичностью и последовательностью изложения учебного материала.

Как правило, в существующей педагогической практике в образовательных организациях создание ЭОР курирует методический совет. В образовательных организациях разрабатываются специальные положения о создании ЭОР [47], [49-51], определяются направления информационного обеспечения учебного процесса. Как правило, от ведущего преподавателя требуется техническое задание, в котором определяется требования объема, структуры и содержания ЭОР. ЭОР относятся к программно-информационным средствам учебного процесса, пользователями которого являются обучающиеся, преподаватели и администрация колледжа. Вне зависимости от содержания и объема ЭОР можно выделить три главных требования пользователей к нему: адекватность содержания, эффективность формы представления, экономическая эффективность.

Адекватность содержания подразумевает соответствие Федеральному государственному образовательному стандарту, полноту представления учебного материала, достаточную для освоения учебной дисциплины междисциплинарного курса, раздела учебной дисциплины поддержку различных форм обучения (очной, очно-заочной и заочной, индивидуальной), соответствие единой методике («от простого к сложному»), соблюдение последовательности представления материалов и т.д., поддержку разных видов учебных занятий (изучение теоретического материала, практические и лабораторные работы), поддержку разных форм контроля знаний (промежуточного, итогового, самоконтроля), учет новейших тенденций в образовании, науке и технике.

Эффективность формы представления информации включает в себя такие требования, как простота и удобство применения, эргономичность,

поддержка активности студента, обеспечение коммуникации с преподавателем и сокурсниками, защита от разрушения, возможность дальнейшей адаптации под изменившиеся условия.

Экономическая эффективность зависит от объема использования ЭОР в учебном процессе таких свойств, как длительный срок эксплуатации, возможность модернизации в процессе эксплуатации, низкая себестоимость и цена, разум конфигурация необходимых аппаратных и программных средств.

При разработке электронных обучающих систем предлагается, в первую очередь использовать программные и аппаратные средства, имеющиеся в образовательной организации. Подготовка текстового и иллюстративного материала для электронных учебных ресурсов производится с использованием лицензионных стандартных программных средств (текстовые и графические редакторы, анимационные программные пакеты, видео- и аудиорекодеры) по выбору автора(ов) ЭОР.

По желанию авторов разработки могут быть использованы другие лицензионные инструментальные программно-технические средства.

Структурирование учебного материала ЭОР оптимально строить на модульном принципе.

Под модулем понимается совокупность знаний и умений, которые позволяют обучаемому выполнять отдельные профессиональные функции, определяемые содержанием Федерального государственного образовательного стандарта. Часть учебного материала в пределах данной темы, имеющую четкое начало и окончание и формирующую конкретные профессиональные знания и умения, выделяется в модульную единицу, которая является наименьшим элементом структуры ЭОР.

Из множества возможных форм структурирования учебного материала предпочтение при экспертизе ЭОР будет отдаваться такому модульному варианту: дисциплина (модуль учебной дисциплины) – тема (модуль А) – раздел (модуль Б) – объект изучения (модульная единица). Базовым элементом такой структуры является четко выделенный объект изучения.

Несколько родственно связанных между собою объектов изучения образуют раздел, несколько разделов – тему, несколько тем – дисциплину.

В рамках предлагаемого модульного принципа структурирования авторы ЭОР должны обеспечить четкость деления учебного материала на составляющие части; однозначность выбора соответствующих форм и средств представления каждой такой части; простоту отбора учебного материала для различных категорий обучаемых путем исключения или дополнительного введения набора объектов изучения.

Создатели ЭОР должны предусмотреть возможность работы в интерактивном режиме, легкость и простоту навигации по структуре ЭОР.

Под навигацией понимается возможность быстро перейти от одной темы к другой, получить необходимую справку, комментарий, просмотреть иллюстрацию (в том числе, видеофильмы, интерактивные анимации, виртуальные модели), быстро найти необходимую информацию, выйти в Интернет, обменяться по электронной почте сообщениями с преподавателем-консультантом. При экспертизе ЭОР, как правило, особое внимание уделяется форме и средствам ведения обучающегося по структуре электронного учебного издания, анализируется качество реализации следующих функций:

- просмотр общей структуры ЭОР, его тем и выбор конкретного объекта изучения из общего списка;
- рекомендации по оптимальной последовательности действий в процессе
- самостоятельного обучения, которые не должны исключать возможности выбора последовательности изучения по усмотрению обучающегося;

- произвольный выбор средств обучения в рамках выбранного объекта изучения (теоретическая часть, подсистема компьютерного тренинга и контроля, подсистема
- моделирования, подсистема экспериментального исследования, подсистема обработки данных.);
- фиксация уже изученного учебного материала с возможностью повторного изучения по желанию обучающегося;
- отображение текущего положения обучающегося в структуре учебной дисциплины с возможностью быстрого перехода на другой уровень. Авторам рекомендуется использовать следующие общепринятые методы навигации по учебному материалу любого курса:
- постраничный доступ к материалу – этот наиболее близкий к традиционному использованию учебных пособий метод используется при получении знаний по какой-либо учебной дисциплине (междисциплинарному курсу) во всех случаях, когда важна последовательность в изложении материала, при этом происходит продвижение по тексту с демонстрацией всех связанных элементов мультимедиа;
- возможность доступа по разделам, темам и подтемам материала важна для понимания логики курса в целом и часто применяется для повторного обращения к информации и при пользовании справочниками;
- поиск по ключевому слову, словосочетанию, строке дает возможность находить требуемые сведения по нужным понятиям, даже не имея представления по логике изложения информации в данной учебной дисциплине (междисциплинарном курсе);
- возможность навигации в текстах по «горячим» словам и связанным темам означает, что при чтении текста пользователь

может выяснить значение выделенных понятий, переместиться в связанный с изложением фрагмент другой темы, конце текста перейти к одной из тем, логически продолжающих прочитанную;

- доступ по элементам мультимедиа, содержащимся в обучающей системе, облегчает поиск нужной информации, поскольку для памяти человека удобнее оперировать со зрительными и звуковыми образами, а не с абстрактными понятиями. В зависимости от организаций материала такими медиаэлементами могут быть таблицы, графики, схемы, рисунки, картографические изображения, анимация, звуковые и музыкальные фрагменты, фотографии, кино- и видеоматериалы, интерактивные элементы.

Особое внимание будет уделено автоматизированному тренингу и контроль при работе с ЭОР. Реализующая эти возможности подсистема контроля знаний должна обеспечивать сохранение результатов тестирования обучающегося в специальном журнальном файле, который позволяет проводить статистический анализ успеваемости по различным признакам. Забегая вперед отметим, что именно это файл и является самым уязвимым и требует наибольшей защиты.

1.3.Критерии оценки электронных образовательных ресурсов

Каждый созданный электронно-образовательный ресурс подлежит оценке. Необходимые критерии не определены нормативно, но основные параметры для оценки качественного и количественного состояния ЭОР существуют.

К ним относятся: охват и содержание, качество и объём, способ фиксации и язык, эргономичность интерфейса, полнота содержания,

интерактивность, программные и технические требования к использованию ЭОР и ряд других.

Для того чтобы измерить необходимый параметр ЭОР, на практике используют различные измерительные шкалы: наименований и классификаций; порядковые; порядковые с интервалом; пропорциональные (количественные).

Стандартное занятие всегда будет отличаться от занятия с применением электронных образовательных ресурсов. С использованием ЭОР можно проводить более интересные лабораторные занятия, практикумы, лекции-дискуссии на основе проблемных ситуаций, так как они полны иллюстраций, презентаций, видео, графической информации, что позволяет делать учебно-проектную деятельность более выразительной и разнообразной. ЭОР сочетается и гармонично дополняет традиционные методы на всех этапах обучения: ознакомление, тренировка, применение, контроль [47, с. 17].

Благодаря ЭОР в домашних условиях обучающиеся могут полноценно выполнить практические занятия, посетить виртуальный музея, провести лабораторный эксперимент. Кроме того, любой обучающийся может самостоятельно провести контроль усвоения собственных знаний, умений, навыков без участия педагога, критерии оценивания уже заложены в ЭОР. ЭОР позволяют не только изучить описание объектов, явлений, процессов, но и работать с ними в интерактивном режиме.

Внедрение в образовательный процесс ЭОР не может исключать традиционные методы обучения, а только гармонично дополнять их. В практике работы преподавателя электронные образовательные ресурсы могут использоваться как в традиционном обучении, так и инициировать применение современных инновационных образовательных технологий.

В основу оценки конструирования моделей электронных образовательных ресурсов нового поколения в образовательном процессе, в условиях традиционного обучения, могут быть положены:

- характер деятельности обучающегося при использовании электронных образовательных ресурсов нового поколения в образовательном процессе;
- характер взаимодействия педагога и обучающегося в условиях использования электронных образовательных ресурсов нового поколения в образовательном процессе [43, 44], [45, 46].

При планировании учебного процесса с использованием электронных образовательных ресурсов, рекомендуется учитывать следующие факты: уровень технического оснащения образовательной организации (от нескольких оборудованных кабинетов информатики по ФГОС, электронной библиотеке, доступа к различным онлайн книгам, журналам, методическим пособиям, до наличия учебного компьютера у каждого обучающегося, включая оснащение проекционным оборудованием, интерактивными досками и т. п.); состояние и степень развитости информационной среды образовательной организации (в том числе обусловливающей использование ИКТ в административном обеспечении образовательного процесса); наличие или отсутствие качественного подключения к Интернет; уровень ИКТ-компетентности работников образовательной организации (педагогов и администраторов); наличие компьютеров дома у обучающихся.

Оценка характеристик качества ЭОР как продукта информационно-коммуникационных технологий должна выполняться на основе требований стандартов ГОСТ Р ИСО/МЭК 12119 ГОСТ Р ИСО/МЭК 12119-2000 Информационная технология (ИТ). Пакеты программ. Требования к качеству и тестирование, ГОСТ Р ИСО 9241-3 ГОСТ Р ИСО 9241-3-2003 Эргономические требования при выполнении офисных работ с использованием видеодисплейных терминалов (ВДТ). Часть 3. Требования к визуальному отображению информации и ГОСТ Р ИСО 9241-8-2007 Эргономические требования при выполнении офисных работ с использованием видеодисплейных терминалов (ВДТ). Часть 8. Требования к отображаемым цветам [1- 3].

Оценка характеристик качества ЭОР с учетом специфики его использования в составе ИОР должна выполняться в соответствии с требованиями стандарта ГОСТ Р 53625-2009 (ИСО/МЭК 19796-1:2005) Информационная технология (ИТ). Обучение, образование и подготовка. Менеджмент качества, обеспечение качества и метрики. Часть 1. Общий подход на основе эталонных критериев качества.

В названном стандарте приведена детализация процессов и подпроцессов. Для целей нашего исследования значимо такое детализированное представление, поскольку при проектировании и разработке ЭОР нам необходимо придерживаться предписанного алгоритма. Приведем его с этапа описания анализа потребностей до описания реализации в таблицах 1, 2,3,4,5.

Таблица 1

Описание процесса "Анализ потребностей"

Категория	*УИ: АП. Процесс: анализ потребностей. Описание: идентификация и описание требований, спроса и ограничений образовательного проекта. Связь: нет*
Подпроцессы/подаспекты	АП.1 Инициирование АП.2 Идентификация заинтересованных сторон АП.3 Определение целей АП.4 Анализ спроса
Цель	Описать потребности и спрос, которые будут учтены в образовательном проекте
Метод	Описание качества функционирования
Результат	Документирование требуемых целей, задач, потребностей и требований к образовательному проекту
Действующие субъекты	Руководитель проекта; специалисты, обучаемые, спонсоры

Метрики/критерии	Указатели
Нормативные документы	ГОСТ Р ИСО 9000

Таблица 2

Описание процесса "Анализ структуры"

Категория	*УИ: АС. Процесс: анализ структуры. Описание: идентификация структуры и контекста образовательного процесса. Связь: АП, КП*
Подпроцессы/подаспекты	АС.1 Анализ внешнего контекста АС.2 Анализ кадровых ресурсов АС.3 Анализ целевых групп АС.4 Анализ институционального и организационного контекстов АС.5 Планирование графика работ и бюджета АС.6 Анализ среды
Цель	Описать соответствующие факторы для образовательного проекта
Метод	Методы эмпирического социального исследования; методы юридического и экономического исследований и анализа
Результат	Документирование и подтверждение соответствующих параметров
Действующие субъекты	Руководитель проекта, специалисты
Метрики/критерии	Проверка правдоподобия, консультации экспертов

Таблица 3

Описание процесса "Концепция/проект"

Категория	*УИ: КП. Название процесса: концепция/проект. Описание: концепция и проект образовательных процессов. Связь: нет*

Подпроцессы/подаспекты	КП.1 Цели обучения КП.2 Концепция содержания КП.3 Дидактическая концепция/методы КП.4 Роли и виды деятельности КП.5 Организационная концепция КП.6 Техническая концепция КП.7 Концепция проекта среды и взаимодействия КП.8 Концепция среды КП.9 Концепция коммуникаций КП.10 Концепция тестов и оценки КП.11 Концепция сопровождения
Цель	Запланировать и разработать концепции для образовательного процесса
Метод	Применение Руководств по разработке
Результат	Концепция и проект образовательных процессов
Действующие субъекты	Консультант, разработчики средств информации

Таблица 4

Описание процесса "Разработка/изготовление"

Категория	*УИ: РИ. Процесс: разработка/изготовление. Описание: реализация концепций. Связь: КП*
Подпроцессы/подаспекты	РИ.1 Реализация контента РИ.2 Реализация проекта РИ.3 Реализация сред РИ.4 Техническая реализация РИ.5 Сопровождение

Цель	Реализовать концепции
Метод	Руководство по реализации
Результат	Образовательные продукты и услуги
Действующие субъекты	Специалисты по информационным технологиям, авторы, разработчики

Таблица 5

Описание процесса "Реализация"

Категория	*УИ: РЕ. Процесс: реализация. Описание: описание реализации технологических компонентов. Связь: нет*
Подпроцессы/подаспекты	РЕ.1 Тестирование ресурсов обучения РЕ.2 Адаптация ресурсов обучения РЕ.3 Приведение в действие ресурсов обучения РЕ.4 Организация применения РЕ.5 Техническая инфраструктура
Цель	Реализовать соответствующие технологические компоненты, используемые в процессе обучения
Метод	Изменение/конфигурирование/управление контентом
Результат	Среда обучения, включая все образовательные ресурсы
Действующие субъекты	Руководитель проекта, менеджер по информационным технологиям
Метрики/критерии	Тестирование бета-версий и системы
Нормативные документы	Валидация программного обеспечения, например, в соответствии с требованиями ИИЭР; ГОСТ Р ИСО 9000

В соответствии с приведенным стандартным описанием могут быть разработаны оценочные экспертные листы, когда отдельному подпроцессу будет сопоставлен показатель, демонстрирующий степень соответствия реализации по приведенной выше детализации ГОСТ.

Один из возможных вариантов экспертных листов был использован нами при оценке разработанного нами ЭОР, листы размещены в Приложении 1, а сопровождающая техническая характеристика «Информационный лист для характеристики педагогического программного средства» в Приложении 2.

1.4. Содержание, структура, экспертная оценка разработанного электронного образовательного ресурса

Для создания ЭОР используются инструментальные средства специализированного (авторские среды) или универсального (системы программирования) характера. Первые рассчитаны на «программирование без программирования», т.е. программа создается путем конструирования и размещения определенных модулей из которых состоит мультимедиа курс, без написания создателем курса сложного машинного кода (именуемого языком программирования). Для работы со вторыми необходимо знание языка программирования.

Для понимания того, какие именно нужны будут функциональные требования разрабатываемого программного педагогического средства сначала ознакомимся с техническим заданием социального заказчика.

Социальным заказчиком выступал ГПБОУ СПО «ЮУрГТК».

Требуемый электронный образовательный ресурс должен был быть разработан для профессионального модуля «ПМ.09 Проектирование, разработка и оптимизация веб-приложений».

Мы провели анализ программы профессионального модуля.

1.1. Область применения примерной программы

Примерная рабочая программа профессионального модуля является частью примерной основной образовательной программы в соответствии с ФГОС СПО

09.02.07 Информационные системы и программирование

код наименование профессии (специальности)

1.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид профессиональной деятельности **Проектирование, разработка и оптимизация веб-приложений** и соответствующие ему профессиональные компетенции:

ПК 9.1. Разрабатывать техническое задание на веб-приложение в соответствии с требованиями заказчика.

ПК 9.2. Разрабатывать веб-приложение в соответствии с техническим заданием.

ПК 9.3. Разрабатывать интерфейс пользователя веб-приложений в соответствии с техническим заданием.

ПК 9.4. Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием.

ПК 9.5. Производить тестирование разработанного веб приложения.

ПК 9.6. Размещать веб приложения в сети в соответствии с техническим заданием.

ПК 9.7. Осуществлять сбор статистической информации о работе веб-приложений для анализа эффективности его работы.

ПК 9.8. Осуществлять аудит безопасности веб-приложения в соответствии с регламентами по безопасности.

ПК 9.9. Модернизировать веб-приложение с учетом правил и норм подготовки информации для поисковых систем.

ПК 9.10. Реализовывать мероприятия по продвижению веб-приложений в сети Интернет.

Дескрипторы сформированности компетенций по разделам профессионального модуля указаны в таблице 6

Таблица 6

Спецификация ПК/ разделов профессионального модуля

Формируемые компетенции	***Название раздела***		
	Действия (дескрипторы)	***Умения***	***Знания***
1	***2***	***3***	***4***
Раздел модуля 1 <u>Проектирование и разработка веб-приложений</u>			
ПК 9.1. Разрабатывать техническое задание на веб-приложение в соответствии с требованиями заказчика	Сбор предварительных данных для выявления требований к веб-приложению. Определение первоначальных требований заказчика к веб-приложению и возможности их реализации. Подбор оптимальных вариантов реализации задач и согласование их с заказчиком. Оформление технического задания.	Проводить анкетирование. Проводить интервьюирование. Оформлять техническую документацию. Осуществлять выбор одного из типовых решений. Работать со специализированным программным обеспечением для планирования времени и организации работы с клиентами.	Инструменты и методы выявления требований. Типовые решения по разработке веб-приложений. Нормы и стандарты оформления технической документации.
1	***2***	***3***	***4***
ПК 9.3. Разрабатывать интерфейс пользователя веб-приложений в соответствии с техническим заданием.	Разрабатывать интерфейс пользователя. Разрабатывать анимационные эффекты	Разрабатывать программный код клиентской части Веб-приложений. Оформлять код программы в соответствии со стандартом кодирования.	Языки программирования и разметки для разработки клиентской части веб-приложений. Принципы работы объектной модели Веб-приложений и браузера.

		Использовать объектные модели Веб-приложений и браузера. Разрабатывать анимацию для Веб-приложений для повышения его доступности и визуальной привлекательности (Canvas).	Технологии для разработки анимации. Способы манипуляции элементами страницы веб-приложения. Виды анимации и способы применения ее.
ПК 9.4. Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием	Устанавливать и настраивать веб-серверы, СУБД для организации работы веб-приложений. Использовать инструментальные средства контроля версий и баз данных. Проводить работы по резервному копированию вебприложений. Выполнять регистрацию и обработку запросов Заказчика в службе технической поддержки.	Подключать и настраивать системы мониторинга работы Веб-приложений и сбора статистики его использования. Устанавливать и настраивать вебсервера, СУБД для организации работы веб-приложений. Работать с системами Helpdesk. Выяснять из беседы с заказчиком и понимать причины возникших аварийных ситуаций с информационным ресурсом. Анализировать и решать типовые запросы заказчиков. Выполнять регламентные процедуры по резервированию данных. Устанавливать прикладное программное обеспечение для резервирования веб-приложений.	Основные показатели использования Веб-приложений и способы их анализа. Регламенты работ по резервному копированию и развертыванию резервной копий веб-приложений. Способы и средства мониторинга работы веб-приложений. Методы развертывания веб-служб и серверов. Принципы организации работы службы технической поддержки. Общие основы решения практических задач по созданию резервных копий.

ПК 9.5. Производить тестирование разработанного веб приложения	Использовать инструментальные средства контроля версий и баз данных, учета дефектов. Тестировать вебприложения с точки зрения логической целостности. Тестировать интеграцию веб-приложения с внешними сервисами и учетными системами.	Выполнять отладку и тестирование программного кода (в том числе с использованием инструментальных средств). Выполнять оптимизацию и рефакторинг программного кода. Кодировать на скриптовых языках программирования; Тестировать веб-приложения с использованием тест-планов. Применять инструменты подготовки тестовых данных. Выбирать и комбинировать техники тестирования вебприложений. Работать с системами контроля версий в соответствии с регламентом использования системы контроля версий. Выполнять проверку веб-приложения по техническому заданию.	Сетевые протоколы и основы webтехнологий. Современные методики тестирования эргономики пользовательских интерфейсов. Основные принципы отладки и тестирования программных продуктов. Методы организации работы при проведении процедур тестирования. Возможности используемой системы контроля версий и вспомогательных инструментальных программных средств для обработки исходного текста программного кода. Регламент использования системы контроля версий. Предметную область проекта для составления тест-планов.
1	***2***	***3***	***4***
Раздел модуля 2 <u>Оптимизация веб-приложений</u>			

ПК 9.7. Осуществлять сбор статистической информации о работе веб-приложений для анализа эффективности его работы.	Реализовывать мероприятия по продвижению веб-приложений в сети Интернет. Собирать и предварительно анализировать статистическую информацию о работе веб-приложений.	Подключать и настраивать системы мониторинга работы Веб-приложений и сбора статистики его использования. Составлять отчет по основным показателям использования Веб-приложений (рейтинг, источники и поведение пользователей, конверсия и др.).	Основные показатели использования Веб-приложений и способы их анализа. Виды и методы расчета индексов цитируемости Веб-приложений (ТИЦ, ВИЦ).
ПК 9.9. Модернизировать веб-приложение с учетом правил и норм подготовки информации для поисковых систем.	Модернизировать веб-приложения для обеспечения доступа к ним поисковых систем.	Модифицировать код веб-приложения в соответствии с требованиями и регламентами поисковых систем. Размещать текстовую и графическую информацию на страницах веб-приложения. Редактировать HTML-код с использованием систем администрирования. Проверять HTMLкод на соответствие отраслевым стандартам.	Особенности работы систем управления сайтами. Принципы функционирования поисковых сервисов и особенности оптимизации Вебприложений под них (SEO). Методы оптимизации веб-приложений под социальные медиа (SMO).
1	***2***	***3***	***4***
ПК 9.10. Реализовывать мероприятия по продвижению веб-приложений в сети Интернет	Реализовывать мероприятия по продвижению веб-приложений в сети Интернет. Собирать и предварительно анализировать статистическую информацию о работе веб-	Подключать и настраивать системы мониторинга работы веб-приложений и сбора статистики его использования. Работать с системами продвижения вебприложений. Публиковать	Принципы функционирования поисковых сервисов. Виды и методы расчета индексов цитируемости веб-приложений (ТИЦ, ВИЦ). Стратегии продвижения вебприложений в

	приложений.	информации о вебприложении в специальных справочниках и каталогах. Осуществлять подбор и анализ ключевых слов и фраз для соответствующей предметной области с использованием специализированных программных средств. Составлять тексты, включающие ссылки на продвигаемый сайт, для размещения на сайтах партнеров	сети Интернет. Виды поисковых запросов пользователей в интернете. Программные средства и платформы для подбора ключевых словосочетаний, отражающих специфику сайта. Инструменты сбора и анализа поисковых запросов.
Раздел модуля 3 <u>Обеспечение безопасности веб-приложений</u>			
ПК 9.8. Осуществлять аудит безопасности веб-приложения в соответствии с регламентами по безопасности.	Обеспечивать безопасную и бесперебойную работу	Осуществлять аудит безопасности веб-приложений. Модифицировать веб-приложение с целью внедрения программного кода по обеспечению безопасности его работы	Источники угроз информационной безопасности и меры по их предотвращению Регламенты и методы разработки безопасных веб-приложений.

Общие компетенции по всем разделам модуля представлены в таблице 7

Таблица 7

Общие компетенции (по всем разделам модуля)

Шифр и наименование компетенций	*Дискрипторы (показатели сформированности)*		*Умения*	*Знания*
	Начальный уровень	*Продвинутый уровень*		
1	***2***	***3***	**4**	**5**

ОК 1.Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Распознавать сложные проблемы в знакомых ситуациях. Выделять сложные составные части проблемы и описывать её причины и ресурсы, необходимые для её решения в целом. Определять потребность в информации и предпринимать усилия для её поиска. Выделять главные и альтернативные источники нужных ресурсов. Разрабатывать детальный план действий и придерживаться его. Качество результата, в целом, соответствует требованиям. Оценивать результат своей работы, выделять в нём сильные и слабые стороны.	Распознавать сложные нерутинные проблемные ситуации в любых условиях. Анализировать сложные проблемные ситуации, выявлять взаимоотношения между действующими факторами, находить скрытые связи и описывать ресурсы, необходимые на каждом этапе решения проблемы. Определять потребность в информации и эффективно находить недостающую в собственном опыте и новых источниках. Выделять все возможные источники нужных ресурсов, в том числе неочевидные. Разрабатывать детальный план действий, оценивать риски на каждом шагу и заранее продумыватьальтернативы.	Распознавать задачу и/или проблему в профессиональном и/или социальном контексте; Анализировать задачу и/или проблему и выделять её составные части; Правильно определить и найти информацию, необходимую для решения задачи и/или проблемы; Составить план действия, Определить необходимые ресурсы; Владеть актуальными методами работы в профессионально й и смежных сферах; Реализовать составленный план; Оценить результат и последствия своих действий (самостоятельно или с помощью наставника).	Знать актуальный профессиональный и социальный контекст, в котором приходится работать и жить; Знать основные источники информации и ресурсов для решения задач и проблем в профессиональном и/или социальном контексте. Знать актуальные стандарты выполнения работ в профессионально й и смежных областях; Знать актуальные методы работы в профессиональной и смежных сферах.

		Привлекать разные источники ресурсов, оценивать их качество и выбирать лучшие. Придерживаться плана, оценивать результат на каждом шаге, применять альтернативные решения в случае неудачи. Результат может превосходить требования к качеству, реализовывать более удачное решение. Оценивать плюсы и минусы полученного результата, своего плана и его реализации, предлагать критерии оценки и рекомендации по улучшению плана.		
ОК 2. Осуществлять поиск, анализ и интерпретацию информации,	Планировать информационный поиск из широкого набора источников, необходимого для выполнения		Определять задачи поиска информации Определять необходимые источники информации Планировать процесс поиска	Номенклатуру информационных источников применяемых в профессиональной деятельности Приемы структурирования информации Формат

необходимой для выполнения задач профессиональной деятельности.	профессиональных задач Проводить анализ полученной информации, выделять в ней главные аспекты Структурировать отобранную информацию в соответствии с параметрами поиска Интерпретировать полученную		Структурировать получаемую информацию Выделять наиболее значимое в перечне информации Оценивать практическую значимость результатов поиска Оформлять результаты поиска	оформления результатов поиска информации
1	***2***	***3***	**4**	**5**
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие	Использовать актуальную нормативноправовую документацию по профессии (специальности) Применять современную научно профессиональную терминологию Определять траекторию профессионального развития и самообразования		Определять актуальность нормативно-правовой документации в профессионально й деятельности	Содержание актуальной нормативно-правовой документации Современная научная и профессиональная терминология Возможные траектории профессионального развития и самообразования
1	2	3	4	5
ОК 4. Работать	Участвовать в деловом		Организовывать работу коллектива	Психология коллектива

в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентам	общении для эффективного решения деловых задач Планировать профессиональную деятельность		и команды. Взаимодействовать с коллегами, руководством, клиентами.	Психология личности Основы проектной деятельности
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	Грамотно устно и письменно излагать свои мысли по профессиональной тематике на государственном языке Проявлять толерантность в рабочем коллективе		Излагать свои мысли на государственном языке. Оформлять документы	Особенности социального и культурного контекста Правила оформления документов.
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих	Понимать значимость своей профессии (специальности) Демонстрировать поведение на основе общечеловечес-ких ценностей.		Описывать значимость своей профессии Презентовать структуру профессионально й деятельности по профессии (специальности)	Сущность гражданско-патриотической позиции Общечеловеческие ценности. Правила поведения в ходе выполнения профессиональной деятельности

ценностей				
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Соблюдать правила экологической безопасности при ведении профессиональной деятельности; Обеспечивать ресурсосбережение на рабочем месте		Соблюдать нормы экологической безопасности Определять направления ресурсосбережения в рамках профессионально й деятельности по профессии (специальности)	Правила экологической безопасности при ведении профессиональной деятельности Основные ресурсызадействованные в профессиональной деятельности Пути обеспечения ресурсосбережения.
1	***2***	***3***	**4**	**5**
ОК 08. Использоватьсредства физическойкультуры для сохранения и укрепления здоровья впроцессепрофессиональной деятельности и поддержание необходимого уровняфизической подготовленности	Сохранять и укреплять здоровье посредством использования средств физической культуры Поддерживать уровень физической подготовленности для успешной реализации профессиональной деятельности		Использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; Применять рациональные приемы двигательных функций в профессиональной деятельности. Пользоваться средствами профилактики перенапряжения характерными для данной профессии (специальности)	Роль физической культуры в общекультурном, профессиональном и социальном развитии человека; Основы здорового образа жизни; Условия профессиональной деятельности и зоны риска физического здоровья для профессии (специальности) Средства профилактики перенапряжения

ОК 09. Использовать информационные технологии в профессиональной деятельности.	Применять средства информатизации и информационных технологий для реализации профессиональной деятельности		Применять средства информационных технологий для решения профессиональных задач. Использовать современное программное обеспечение	Современные средства и устройства информатизации Порядок их применения и программное обеспечение в профессиональной деятельности
1	***2***	***3***	**4**	**5**
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	Применять в профессиональной деятельности инструкций на государственном и иностранном языке. Вести общение на профессиональные темы		Понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы участвовать в диалогах на знакомые общие и профессиональные темы, строить простые высказывания о себе и о своей профессиональной деятельности, кратко обосновывать и объяснить свои действия (текущие и планируемые), писать простые связные сообщения на знакомые или интересующие профессиональные	Правила построения простых и сложных предложений на профессиональные темы, основные общеупотребительные глаголы (бытовая и профессиональная лексика), лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности, особенности произношения, правила чтения текстов профессиональной направленности

			темы	
ОК 11. Планировать предпринимательскую деятельность в профессиональной сфере.	Определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности. Составлять бизнес-план. Презентовать бизнес-идею. Определять источники финансирования. Применять грамотные кредитные продукты для открытия дела		Выявлять достоинства и недостатки коммерческой идеи. Презентовать идеи открытия собственного дела в профессиональной деятельности. Оформлять бизнес-план. Рассчитывать размеры выплат по процентным ставкам кредитования	Основы предпринимательской деятельности Основы финансовой грамотности Правила разработки бизнес-планов Порядок выстраивания презентации Кредитные банковские продукты

Общие и профессиональные компетенции, указанные во ФГОС СПО и данной примерной программе были дополнены в рабочей программе профессионального модуля на основе:

- анализа требований соответствующих профессиональных стандартов;

- анализа актуального состояния и перспектив развития регионального рынка труда;

- обсуждения с заинтересованными работодателями.

Мы сосредоточили свое внимание на разделе 1 профессионального модуля «Проектирование и разработка веб-приложений», в котором формируется компетенция ПК 9.2. Разрабатывать веб-приложение в соответствии с техническим заданием (см. таблицу 6) и от студента требуется после освоения этого раздела уметь разрабатывать программный код

приложений, кодировать на языках веб-программирования, использовать объектные модели Веб-приложений и браузера, использовать открытые библиотеки (framework), использовать выбранную среду программирования и средства системы, а также знания языков программирования и разметки для разработки клиентской и серверной части веб-приложений, принципов работы объектной модели веб-приложений и браузера, особенностей отображения веб-приложений в размерах рабочего пространства устройств и др.

Мы разработали электронный практикум по языку программирования PHP, используя программное обеспечение PuTTY (клиент SSH и telnet), изначально разработанное Саймоном Тэтхэмом для платформы Windows. PuTTY - это программное обеспечение с открытым исходным кодом, которое поддерживается группой добровольцев, а также нами было использован Notepad ++ - бесплатный редактор исходного кода и замена блокнота, поддерживающая несколько языков. Работает в среде MS Windows, его использование регулируется лицензией GPL .

Основанный на мощном компоненте редактирования Scintilla , Notepad ++ написан на C ++ и использует чистый Win32 API и STL, что обеспечивает более высокую скорость выполнения и меньший размер программы. Notepad ++ оптимизирует как можно больше процедур без потери удобства. При использовании меньшей мощности процессора ПК может снизить скорость и снизить энергопотребление, что приведет к более экологичной среде.

Вся база заданий для практикума представлена в Приложении 1 и частично заимствована нами из учебника « PHP Собеседование в вопросах и ответах» Андрея Шевченко, который распространяется на условиях лицензии Creative Commons Attribution-NonCommercial-ShareAlike (Атрибуция – Некоммерческое использование – С сохранением условий) 3.0 Непортированная.

Интерфейс представлен на скриншотах – рисунки 2-5, свободное поле служит для ввода либо ответов, либо программного кода.

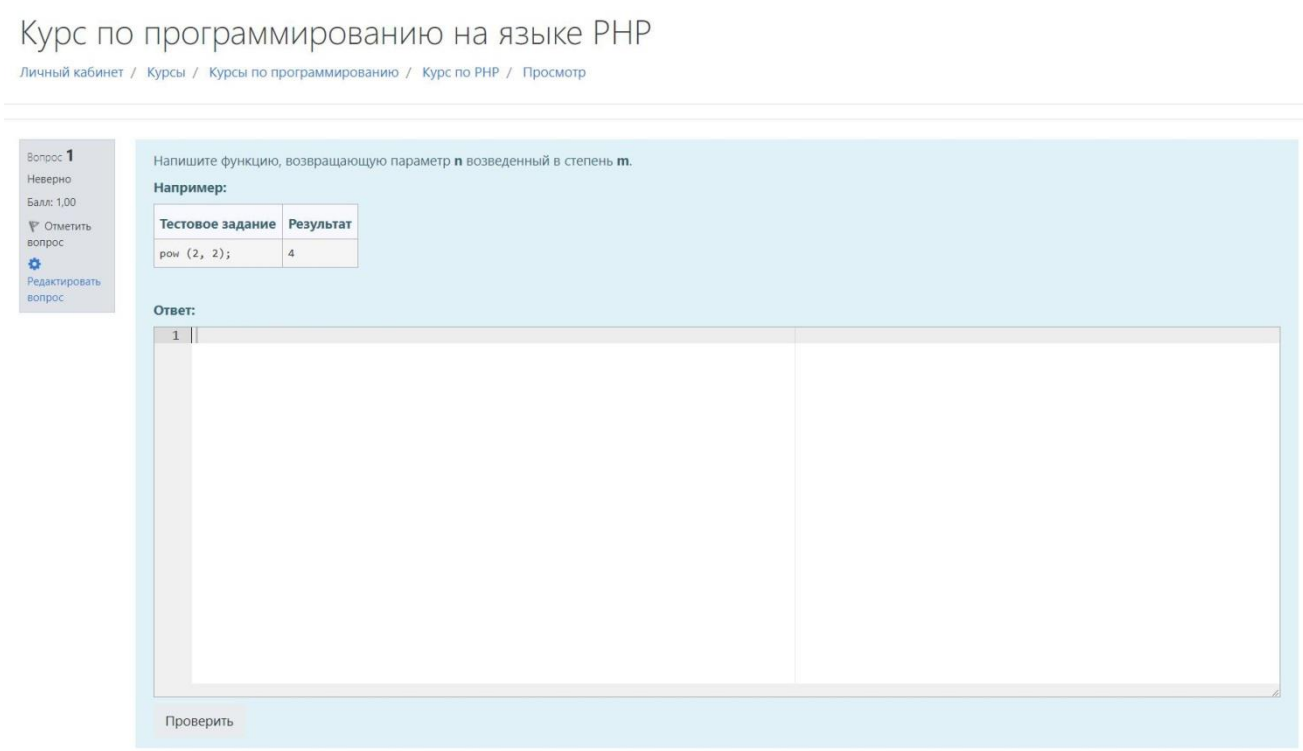

Рисунок 2

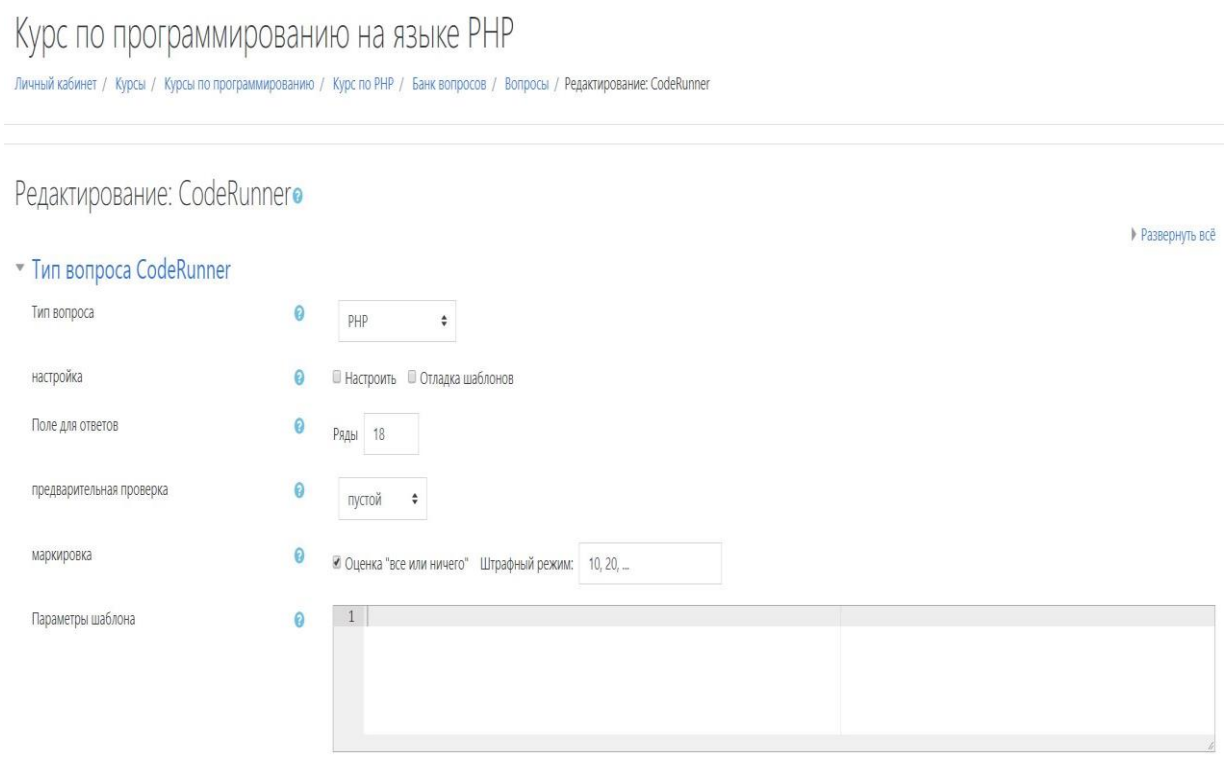

Рисунок 3

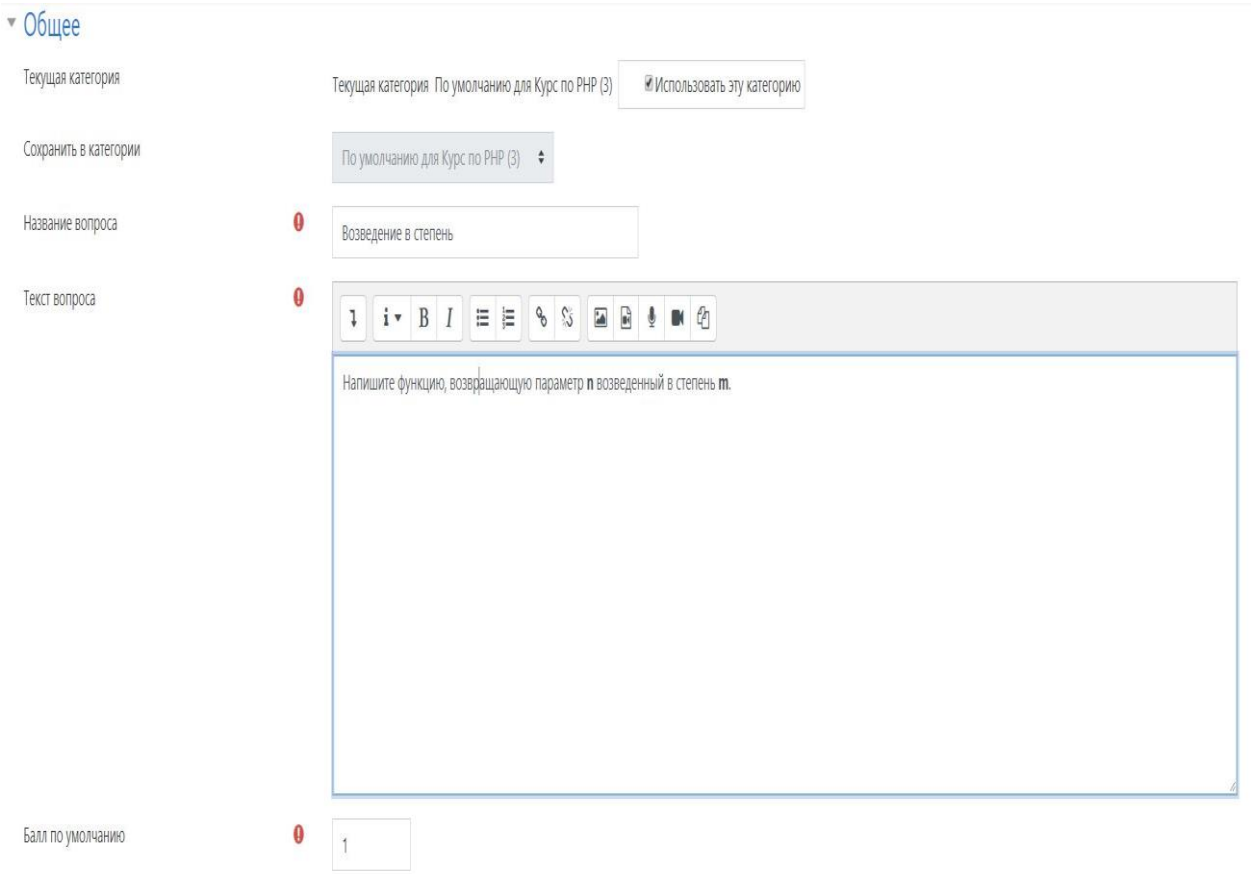

Рисунок 4

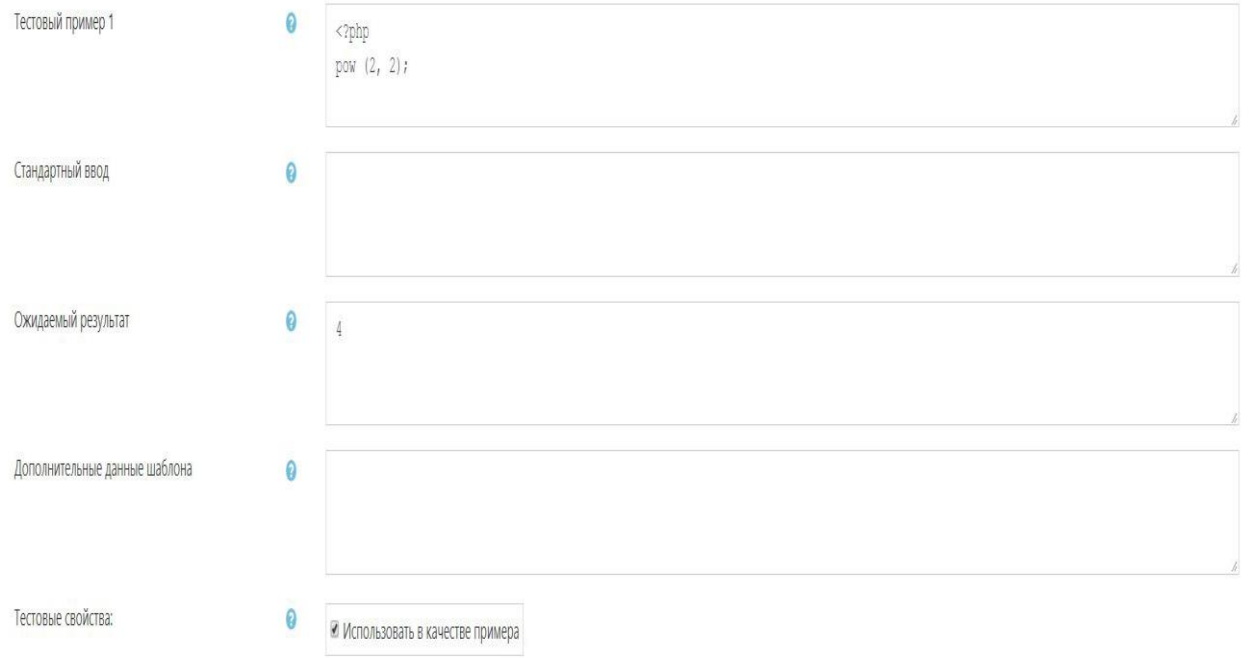

Рисунок 5

Разработанный ЭОР прошел экспертную оценку – преподавателями спецдисциплин в области IT-технологий ГБПОУ «ЮУрГТК».

Оценочный лист (образец представлен в Приложении 2) оформлен в виде таблицы, включающей четыре группы критериев:

1) технический критерий. Он подразумевает корректность работу программы вне зависимости от операционной системы, типовых системных требований

2) эргономический критерий. В этом разделе оцениваются сервис пользователя и эргономичность представления информации на экране, соответствие контрастности ГОСТ.

3) педагогический критерий. Здесь оцениваются: цели использования педагогического программного продукта; методы обучения с использованием ЭОР; психолого-педагогическое воздействие - формирование мышления, учебного опыта самостоятельного приобретения знаний, умений, навыков, приобретение учебного опыта экспериментально-исследовательской деятельности и ряд других критериев;

4) критерий интерактивности – возможности оперативного получения обратной связи обучающимся

Кроме описанных криетриев оценочный лист содержит:

а) итоговую оценку;

б) итоговое заключение эксперта - обобщенное впечатление, его особенности.

Результаты экспертной оценки ЭОР представлены в табл. 8.

Таблица 8

Результаты экспертной оценки

№ п/п	Эксперт / Уровень	К.В.И.	Ш.В.А	Г.Е.А.	Ш.О.Н.	Л.А.В.	Среднее значение
1	Технический	5	4,8	4,6	4,2	4	4,5
2	Эргономический	4,2	3,8	4	4,6	4,2	4,1
3	Педагогический	3,9	4	4,4	4,8	3,6	4,1
4	Интерактивности	4,6	5	4,8	4	4,3	4,5

По данным табл. 8 построены диаграммы, представленные на рис.6

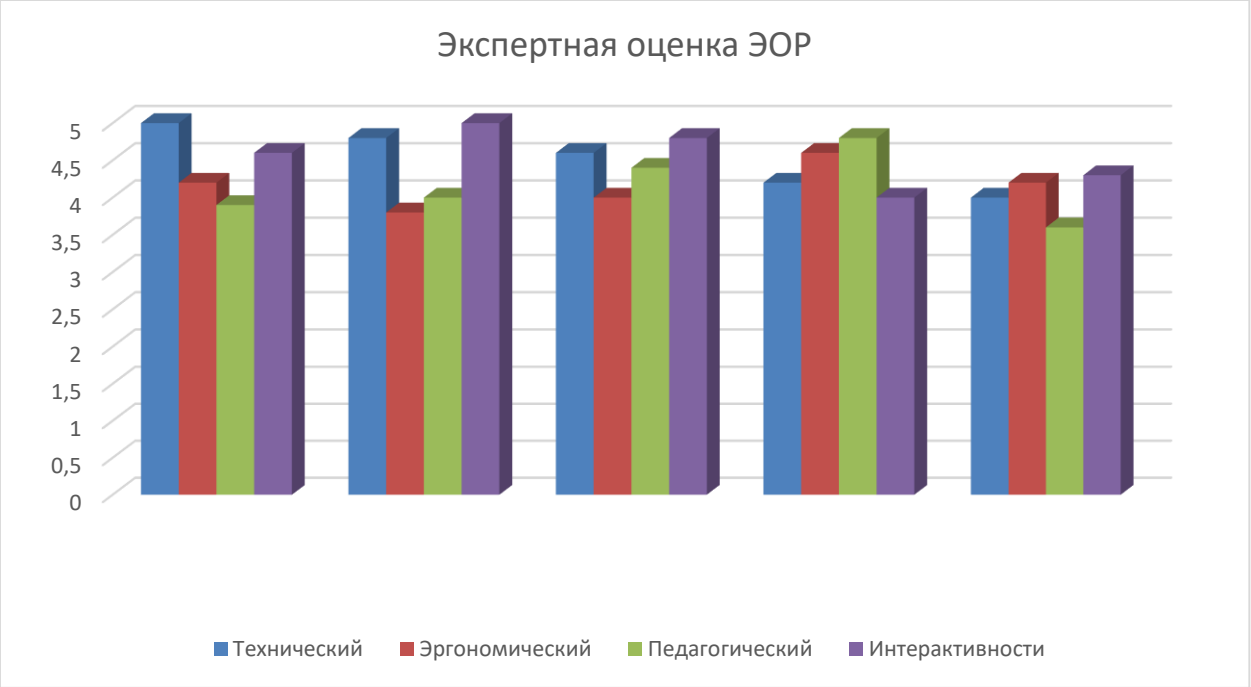

Рисунок 6– Результаты экспертной оценки программного продукта

Оценка ЭОР экспертами показала, что программный продукт выполнен на хорошем уровне и соответствует основным требованиям качества электронного образовательного ресурса, подтверждены: способность применения в реальном учебном процессе и достижимость поставленных педагогических целей.

Содержание ЭОР представлено в Приложение 1.

Выводы по I главе

Электронные образовательные ресурсы являются содержательной частью информационной образовательной системы любой образовательной организации, в том числе и, в первую очередь, образовательной организации среднего профессионального образования (далее – СПО).

Дидактические возможности ЭОР многообразны: повышение эффективности обучения и качества знаний обучающихся; развитие познавательной активности; повышение интереса к изучаемому предмету; развитие аналитического мышления; формирование навыков работы с компьютером; формирование навыков коллективной работы; формирование навыков самостоятельного исследования и другие.

Этапы создания ЭОР регламентированы соответствующими ГОСТами, а также внутренними локальными актами образовательных организаций. В любом случае присутствует следующая последовательность этапов: этап выявления потребности в создании ЭОР, этап проектирования структуры и отбора содержания; этап разработки, этап апробации и отладки. После чего ЭОР начинает применяться в образовательной практике.

Наряду с традиционными критериями оценки ЭОР, такими как соответствие программе обучения, научная обоснованность представляемого материала, соответствие единой методике, отсутствие фактографических ошибок, аморальных, неэтичных компонентов, соответствие требованиям ГОСТ по технологическим и эргономическим характеристикам применяются также и инновационные: обеспечение всех компонентов образовательного процесса (получение информации, практические занятия, контроль учебных достижений); интерактивность, возможность удаленного (дистанционного), полноценного обучения и ряд других.

ГЛАВА 2. РЕАЛИЗАЦИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ НА ПРИМЕРЕ ГПБОУ «ЮУРГТК»

2.1. Основные направления политики информационной безопасности ГПБОУ «ЮУрГТК»

В современных условиях тотальной информатизации все очевидней становится противоречие между запросами обучающихся и возможностями использования информационных ресурсов (далее – ИР), которые предлагаются образовательными организациями. Ресурсы информационно-образовательной среды должны быть не только доступны, но и защищены, то есть от администрации образовательной организации требуется к тому же обеспечить их целостность и конфиденциальность.

Для решения этих актуальных задач образовательные организации разрабатывают концепции информационной безопасности (далее-ИБ), в которых описывают меры, методы и объекты защиты.

Рассмотрим и проанализируем существующий опыт создания и реализации таких концепций для целей защиты информации.

Как правило, структура такой концепции включает в себя следующие тематические разделы:

- нормативно-правовая база
- понятийный аппарат
- описание объектов защиты
- принципы реализации защиты
- административные и организационные меры и методы
- программно-аппаратные меры и методы

Нормативно-правовой базой выступают федеральные законы, такие как ФЗ от 27 июля 2006г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [14], ФЗ от 27.07.2006 №152-ФЗ «О персональных данных» [15], ФЗ от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [16], нормативно-методические документы ФСТЭК и ФСБ, а также стратегические документы РФ, определяющие политику государства в области защиты информации и конституционных прав граждан: Доктрина информационной безопасности Российской Федерации [11], Концепция общественной безопасности в РФ как правовая мера безопасности образовательных учреждений (организаций) [13] и ряд других.

Понятийный аппарат концепций практически полностью совпадает с понятийным аппаратом названных правовых актов.

К объектам защиты образовательные организации как правило относят персональные данные (далее – ПДн) сотрудников и обучающихся, и именно этот информационный ресурс считают наиболее ценным и подлежащим тщательной защите. Однако, такую позицию нельзя считать правильной, поскольку защита необходима и для электронных образовательных ресурсов и для информации о материально-технической базе и структуре информационной системы образовательной организации/

Как справедливо указывает Шемяков О.А. в [46], образовательные организации должны обеспечить следующие направления защиты:

организацию защищенного доступа к образовательным материалам и системам из любой точки мира;

- защиту информации ограниченного доступа (персональные данные, коммерческая тайна и т.п.) и защита интеллектуальной собственности;

• выполнение требований законодательства в области информационной безопасности (защита персональных данных, защита прав на интеллектуальную собственность, защита детей от негативной информации).

Принципы реализации защиты разработаны в теории защиты информации [22], [29], [48] и существенно не различаются в концепциях различных образовательных организаций: системность, комплексность, непрерывность, разумная достаточность, открытость алгоритмов защиты, простота применения защиты, минимизация полномочий, персональная ответственность.

Организационные меры состоят из мер административного уровня и процедурных мер защиты информации. Основой мер административного уровня является совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Как показал анализ интернет-сайтов образовательных организаций, а нами был проведен просмотр 60 сайтов (от детских садов до вузов), лишь небольшое количество образовательных организаций - менее 10% из нашего мониторинга, имеют документально оформленную политику информационной безопасности, в которой были бы представлены: политика защиты от НСД к информации; политика предоставления доступа пользователей в информационной систем; политика управления паролями; политика предоставления доступа к ресурсам сети Интернет; политика управления доступом к информационным ресурсам ИС предприятия; политика использования электронной почты и другие политехнические и программные положения использования ИР учебного заведения, как предлагается сделать для предприятия.

В большей степени проработаны вопросы программно-аппаратной защиты. Считаем, что это объясняется мощной нормативно-методической

базой ФСТЭК и ФСБ, вследствие чего, даже при условии не прохождения образовательной организацией процедуры аттестации, как объекта информатизации, уровень подготовки специалистов по защите информации является достаточно высоким [46,48].

Помимо описанных разделов в концепцию информационной безопасности часто включаются порядок категорирования защищаемой информации, распределение ответственности и порядок взаимодействия, модели нарушителей, что, безусловно, способствует усилению уровня защищенности данной образовательной организации.

Детальное и подробное описание системы защиты информации, изложенное в концепции информационной безопасности организации является требованием времени и необходимым условием его защищенности [13].

Концепция ИБ как правило фиксируется в «Политике информационной безопасности организации», являющейся набором правил и локальных документов, которые регулируют управление, защиту и распределение информации в организации. Часто политика информационной безопасности трактуется как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса. Результатом политики является высокоуровневый документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Данный документ представляет методологическую основу практических мер (процедур) по реализации информационной безопасности и содержит следующие группы сведений:

1. Основные положения информационной безопасности.
2. Область применения.
3. Цели и задачи обеспечения информационной безопасности.
4. Распределение ролей и ответственности.

5. Общие обязанности.

Основные положения определяют важность обеспечения информационной безопасности, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

Областью применения политики безопасности являются основные активы и подсистемы автоматизированной информационной системы организации (далее – АИС), подлежащие защите. Типовыми активами являются программно-аппаратное и информационное обеспечение АИС, персонал, в отдельных случаях – информационная инфраструктура организации.

Цели, задачи, критерии обеспечения ИБ вытекают из особенностей информационных активов образовательной организации.

Типовые цели описаны в ГОСТ Р 57628-2017 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности [3-5], которому, в свою очередь, предшествовал ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий [7-9]. Настоящий стандарт устанавливает основные понятия и принципы оценки безопасности ИТ, а также определяет общую модель оценки, которой посвящены различные части стандарта, предназначенного в целом для использования в качестве основы при оценке характеристик безопасности продуктов ИТ.

В названных стандартах представлен краткий обзор и описание всех частей системы обеспечения информационной безопасности, определены термины, установлено основное понятие объекта оценки (ОО), контекста оценки, описана целевая аудитория, которой адресованы критерии оценки

ИБ, а также предложены меры и способы реализации ИБ, которые доводятся и конкретизируются в каждой организации.

Очевидно, что каждая образовательная организация формулирует собственную политику ИБ в соответствии со спецификой и особенностями иерархии организационной структуры, имеющейся инфраструктурой, существующими традициями, требованиями внутренних локальных актов и другими нюансами.

Политика безопасности затрагивает всех пользователей компьютеров в организации, поэтому важно решить так называемые политические вопросы наделения всех категорий пользователей соответствующими правами, привилегиями и обязанностями. Для этого определяется круг лиц, имеющий доступ к подсистемам и сервисам АС. Для каждой категории пользователей описываются правильные и неправильные способы использования ресурсов – что запрещено и разрешено. Здесь специфицируются уровни и регламентация доступа различных групп пользователей. Следует указать, какое из правил умолчания на использование ресурсов принято в организации, а именно:

Права и обязанности пользователей определяются применительно к безопасному использованию подсистем и сервисов АС. При определении прав и обязанностей администраторов следует стремиться к некоторому балансу между правом пользователей на тайну и обязанностью администратора контролировать нарушения безопасности.

Важным элементом политики является распределение ответственности. Политика не может предусмотреть всего, однако, она должна для каждого вида проблем найти ответственного.

Обычно выделяются несколько уровней ответственности. На первом уровне каждый пользователь обязан работать в соответствии с политикой безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех

подозрительных ситуациях. Системные администраторы отвечают за защиту соответствующих информационно-вычислительных подсистем. Администраторы сетей должны обеспечивать реализацию организационно-технических мер, необходимых для проведения в жизнь политики безопасности АС. Руководители подразделений отвечают за доведение и контроль положений политики безопасности.

С практической точки зрения, политику безопасности целесообразно разделить на несколько уровней. Как правило, выделяют два-три уровня.

Верхний уровень носит общий характер и определяет политику организации в целом. Здесь основное внимание уделяется: порядку создания и пересмотра политики безопасности; целям, преследуемым организацией в области информационной безопасности; вопросам выделения и распределения ресурсов; принципам технической политики в области выбора методов и средств защиты информации; координированию мер безопасности; стратегическому планированию и контролю; внешним взаимодействиям и другим вопросам, имеющим общеорганизационный характер.

На указанном уровне формулируются главные цели в области информационной безопасности (определяются сферой деятельности предприятия): обеспечение конфиденциальности, целостности и/или доступности.

Средний уровень политики безопасности выделяют в случае структурной сложности организации либо при необходимости обозначить специфичные подсистемы организации. Это касается отношения к перспективным, еще не достаточно апробированным технологиям. Например, использование новых сервисов Интернет, организация связи и обработка информации на домашних и портативных компьютерах, степень соблюдения положений компьютерного права и др. Кроме того, на среднем уровне политики безопасности могут быть выделены особо значимые

контуры АС организации, например, обрабатывающие секретную или критически важную информацию.

За разработку и реализацию политики безопасности верхнего и среднего уровней отвечают руководитель службы безопасности, администраторы безопасности АС, администратор корпоративной сети.

Нижний уровень политики безопасности относится к конкретным службам или подразделениям организации и детализирует верхние уровни политики безопасности. Данный уровень необходим, когда вопросы безопасности конкретных подсистем требуют решения на управленческом, а не только на техническом уровне.

На данном уровне определяются конкретные цели, частные критерии и показатели информационной безопасности, определяются права конкретных групп пользователей, формулируются соответствующие условия доступа к информации и т. п. Здесь из конкретных целей выводятся (обычно формальные) правила безопасности, описывающие, кто, что и при каких условиях может делать или не может. Более детальные и формальные правила упростят внедрение системы и настройку средств ОБИ.

На этом уровне описываются механизмы защиты информации и используемые программно-технические средства для их реализации (в рамках, конечно, управленческого уровня, но не технического).

За политику безопасности нижнего уровня отвечают системные администраторы.

В рамках разработки политики безопасности проводится анализ рисков (risk analysis). Это делается с целью минимизации затрат на обеспечение информационной безопасности. Напомним, что основной принцип безопасности – затраты на средства защиты не должны превышать стоимости защищаемых объектов. При этом если политика безопасности оформляется в виде высокоуровневого документа, описывающего общую стратегию, то

анализ рисков (как приложение) оформляется в виде списка активов, нуждающихся в защите.

Примерный перечень вопросов, входящих в состав политики безопасности информационных технологий организации определен в ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий» [8]:

1 Введение

1.1 Общий обзор

1.2 Область применения и цель политики обеспечения безопасности информационных технологий

2 Цели и принципы обеспечения безопасности

2.1 Цели

2.2 Принципы

3 Организация и инфраструктура безопасности

3.1 Ответственность

3.2 Основные направления политики обеспечения безопасности

3.3 Регистрация инцидентов нарушения безопасности

4 Анализ риска и стратегия менеджмента в области обеспечения безопасности ИТ

4.1 Введение

4.2 Менеджмент и анализ риска

4.3 Проверка соответствия мер обеспечения безопасности предъявляемым требованиям

5 Чувствительность информации и риски

5.1 Введение

5.2 Схема маркировки информации

5.3 Общий обзор информации в организации

5.4 Уровни ценности и чувствительности информации в организации

5.5 Общий обзор угроз, уязвимых мест и рисков

6 Безопасность аппаратно-программного обеспечения

6.1 Идентификация и аутентификация

6.2 Контроль доступа

6.3 Журнал учета использования ресурсов и аудит

6.4 Полное стирание

6.5 Программное обеспечение, нарушающее нормальную работу системы

6.6 Безопасность ПК

6.7 Безопасность компактных портативных компьютеров

7 Безопасность связи

7.1 Введение

7.2 Инфраструктура сетей

7.3 Интернет

7.4 Криптографическая аутентификация и аутентификация сообщений

8 Физическая безопасность

8.1 Введение

8.2 Размещение оборудования

8.3 Безопасность и защита зданий

8.4 Защита коммуникаций и систем обеспечения энергоносителями в зданиях

8.5 Защита вспомогательных служб

8.6 Несанкционированное проникновение в помещения

8.7 Доступность ПК и рабочих станций

8.8 Доступ к магнитным носителям информации

8.9 Защита персонала

8.10 Противопожарная защита

8.11 Защита от воды (жидкой среды)

8.12 Обнаружение опасностей и сообщение о них

8.13 Защита системы освещения

8.14 Защита оборудования от кражи

8.15 Защита окружающей среды

8.16 Управление услугами и техническим обслуживанием

9 Безопасность персонала

9.1 Введение

9.2 Условия найма персонала

9.3 Осведомленность и обучение персонала в области безопасности

9.4 Служащие

9.5 Контракты с лицами, проводящими самостоятельную работу

9.6 Привлечение третьих сторон

10 Безопасность документов и носителей информации

10.1 Введение

10.2 Безопасность документов

10.3 Хранение носителей информации

10.4 Ликвидация носителей информации

11 Обеспечение непрерывности деловой деятельности, включая планирование действий при чрезвычайных ситуациях и восстановлении после аварий, стратегии и план (планы)

11.1 Введение

11.2 Запасные варианты

11.3 Стратегия обеспечения бесперебойной работы организации

11.4 План (планы) обеспечения бесперебойной работы организации

12 Надомная работа

13 Политика аутсортинга

13.1 Введение

13.2 Требования безопасности

14 Управление изменениями

14.1 Обратная связь

14.2 Изменения в политике обеспечения безопасности

14.3 Статус документа

Анализ нормативных документов ЮУрГТК показал, что общей концепции ИБ не разработано, а есть отдельные документы, относящиеся к верхнему, среднему и нижнему уровням безопасности.

К верхнему уровню политики ИБ относится «Программа развития профессиональной образовательной организации СПО на 2014-2018 гг», в котором названа задача обеспечения комплексной безопасности образовательного процесса [52]

К среднему уровню политики ИБ следует отнести следующие документы: «Положение об организации работы по охране труда, обеспечению безопасности образовательного процесса в ГБПОУ «Положение об обработке и защите персональных данных в ГБПОУ «Южно-Уральский государственный технический колледж», «Политика в отношении персональных данных в ГБПОУ «Южно-Уральский государственный технический колледж»[52]. В перечисленных документах определены основные направления по защите персональных данных, о реализации комплексной безопасности образовательного процесса.

К нижнему уровню политики ИБ относятся непосредственно должностные обязанности системных администраторов, специалистов по безопасности и инженеров - информатизационного центра.

Однако, несмотря на то, что в ГБПОУ ЮУрГТК разработан пакет документов, определяющий политику безопасности организации, отсутствует регламентация действий по использованию ЭОР, как важной составляющей информационных ресурсов образовательного процесса, нет четкого алгоритма формирования ролей доступа к ЭОР, что является уязвимостью информационной системы, также не определен единый порядок действий при проведении промежуточной или итоговой аттестации.

2.2. Анализ защищенности ЭОР в ГБПОУ ЮУрГТК в рамках реализации политики информационной безопасности образовательной организации

Проведем анализ защищенности ЭОР в ГБПОУ ЮУрГТК, опираясь на ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий» [9,10], приложения C, D, E ГОСТа.

ЭОР безусловно значимый информационный актив, и требования обеспечения для этого ресурса конфиденциальности, целостности и доступности распространяется на ЭОР.

Из перечня типичных видов угроз (приложение C) нами были определены следующие угрозы, которые имеют место быть в ЮУрГТК:

1. Несанкционированное использование носителей данных
2. Ухудшение состояния носителей данных
3. Ошибка обслуживающего персонала
4. Ошибка при обслуживании
5. Программные сбои
6. Использование программного обеспечения несанкционированными пользователями
7. Использование программного обеспечения несанкционированным способом
8. Нелегальное проникновение злоумышленников под видом санкционированных пользователей
9. Незаконное использование программного обеспечения
10. Вредоносное программное обеспечение
11. Незаконный импорт/экспорт программного обеспечения
12. Ошибка операторов
13. Ошибка при обслуживании

14. Доступ несанкционированных пользователей к сети
15. Использование сетевых средств несанкционированным способом
16. Технические неисправности сетевых компонентов
17. Сбои в функционировании услуг связи (например сетевых услуг)
18. Недостаточная численность персонала
19. Ошибки пользователей
20. Ненадлежащее использование ресурсов

Консультации с техническим персоналом ГПБОУ «ЮУрГТК», интервьюирование, позволило выявить наиболее значимые из представленных.

Поскольку обеспечение безопасности по аспектам технического состояния корпоративной сети осуществляют сотрудники информатизационного центра, а также лаборатории технического обеспечения. Из статистики технических отделов следует, что угрозы 3,4,5,12, 13, 16, 17, 18 составляют всего лишь несколько процентов, из чего следует, что при оценке рисков угроз ИБ ЭОР этими угрозами можно пренебречь.

Оставшиеся угрозы можно распределить по нескольким группам. Мы сгруппировали их следующим образом:

I. Злонамеренные действия пользователей (к ним мы отнесли 1, 6, 7, 8, 9, 11, 14),
II. Недостатки оборудования и ПО (к ним мы отнесли 2, 10)
III. Ненадлежащее использование ресурсов (к ним мы отнесли 15, 19, 20.

Из выделенных групп угроз наибольшую опасность для ЭОР представляет I группа.

Из приложения D ГОСТ [10] были выбраны уязвимости, относящиеся к I группе угроз ИБ ЭОР: несовершенство механизмов идентификации и аутентификации; отсутствие, либо нерегулярность аудиторской проверки системы ИБ; незащищенные таблицы паролей, либо неэффективное

управление паролями (легко определяемые пароли, хранение в незашифрованном виде, недостаточно частая замена паролей); неправильное присвоение прав доступа; отсутствие регистрации конца сеанса при выходе с рабочей станции (возможна, например, угроза использования программного обеспечения несанкционированными пользователями).

Воспользуемся методикой ранжирования угроз по мерам риска (приложение Е). Для установления пошаговой взаимозависимости между факторами воздействия (ценность актива) и вероятностью возникновения угрозы (с учетом аспектов уязвимости) может использоваться матрица или таблица. Мы использовали таблицу, нумерацию угроз оставили прежде, угрозы взяты из группы I, как наиболее значимой по угрозам.

Первый шаг — оценка воздействия (ценности актива) по заранее определенной шкале, например от 1 до 5, для каждого подвергаемого угрозе актива (колонка b в таблице 2). Рассматриваемый актив – ЭОР, варьируются только угрозы.

Второй шаг — оценка вероятности возникновения угрозы по заранее определенной шкале, например от 1 до 5, для каждой угрозы (колонка с в таблице 2).

Третий шаг — расчет мер риска умножением результатов первых двух шагов (b — c).

На заключительном этапе проранжируем уязвимости по значению коэффициента «подверженности воздействиям». Все сведения представлены в таблице 9.

Таблица 9

Анализ рисков

Дескриптор угроз a	Оценка воздействия (ценности актива - ЭОР) b	Вероятность возникновения угрозы C	Мера риска d	Ранг угрозы e
Угроза 1	2	2	4	5
Угроза 6	2	2	4	5
Угроза 7	5	2	10	3
Угроза 8	5	4	20	1
Угроза 9	2	3	6	4
Угроза 11	2	3	6	4
Угроза 14	4	4	16	2

Обоснование оценки воздействия и вероятности угроз было получено также путем интервьюирования специалистов по безопасности и определение средней целочисленной оценки.

Таким образом, из проведенного анализа следует, что наибольшие риски имеются при реализации угроз 8 и 14 - нелегальное проникновение злоумышленников под видом санкционированных пользователей и доступ несанкционированных пользователей к сети. Необходимо учесть результаты проведенного анализа при разработке мер информационной защиты.

Выводы по 2 главе

Основные направления политики информационной безопасности ГПБОУ «ЮУрГТК» на момент проведения нашего исследования определены во внутренних локальных актах: «Положение об официальном сайте ГБПОУ «ЮУрГТК», «Положение об обработке и защите персональных данных в ГБПОУ «ЮУрГТК», «Политика в отношении обработки персональных данных в ГБПОУ «ЮУрГТК», «Положение об организации работы по охране труда, обеспечению безопасности образовательного процесса в ГБПОУ «ЮУрГТК», «Правила пользования библиотекой».

Анализ защищенности ЭОР в ГПБОУ «ЮУрГТК» в рамках реализации политики информационной безопасности образовательной организации был проведен на основе ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Мы воспользовались методикой ранжирования угроз по мерам риска, когда для установления пошаговой взаимозависимости между факторами воздействия (ценности актива) и вероятностью возникновения угрозы составляется матрица угроз, в которой ранжируются угрозы по коэффициентам, являющимся усредненными оценками экспертов. Экспертами выступали сотрудники информатизационного центра ГПБОУ «ЮУрГТК» в процессе их интервьюирования.

Анализ показал, что наибольшие риски имеются при реализации угроз нелегального проникновения злоумышленников под видом санкционированных пользователей и доступа несанкционированных пользователей к сети.

ГЛАВА 3 МЕРЫ ПО ОБЕСПЕЧЕНИЮ ТРЕБОВАНИЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГПБОУ «ЮУРГТК»

3.1.Развертывание изолированной среды (песочницы)

С учетом проведенного анализа защищенности электронных образовательных ресурсов, выявленных тенденций обеспечения информационной безопасности информационных ресурсов мы реализовали так называемую «песочницу», используя плагин CodeRunner (V3.3.0) для Moodle.

Песочница — специально выделенная среда для безопасного исполнения компьютерных программ. Обычно представляет собой жёстко контролируемый набор ресурсов для исполнения гостевой программы — например, место на диске или в памяти. Доступ к сети, возможность сообщаться с главной операционной системой или считывать информацию с устройств ввода обычно либо частично эмулируют, либо сильно ограничивают. Песочницы представляют собой пример виртуализации [21].

Повышенная безопасность исполнения кода в песочнице зачастую связана с большой нагрузкой на систему — именно поэтому некоторые виды песочниц используют только для неотлаженного или подозрительного кода.

CodeRunner - это плагин для Moodle. Наибольшее распространение CodeRunner получила в курсах программирования, где студентов просят написать программный код в соответствии с какой-либо спецификацией, и этот код затем оценивается путем запуска его в серии тестов. Вопросы CodeRunner также использовались в других областях компьютерной науки и техники для оценки вопросов, в которых возможно много разных правильных ответов, и для оценки правильности должна использоваться программа.

CodeRunner и его предшественники *pycode* и *ccode* используются в университетской практике, выполняя более миллиона заявок на вопросы

студентов на Python, C, JavaScript, PHP, Octave и Matlab. Другие курсы с использованием Moodle / CodeRunner включают в себя:

1. EMTH171 Математическое моделирование и вычисления
2. SENG02 Software Engineering I
3. COSC261 Формальные языки и компиляторы
4. COSC367 Вычислительный интеллект
5. ENCE360 Операционные системы
6. SENG365 Web Computing Architecture

CodeRunner в настоящее время поддерживает Python2 (считается устаревшим), Python3, C, C ++, Java, PHP, JavaScript (NodeJS), Octave и Matlab. Архитектура позволяет легко модифицировать ее и на другие языки.

CodeRunner можно безопасно использовать на установленном сервере Moodle, при условии, что программное обеспечение песочницы, в котором выполняется код («Jobe»), установлено на отдельном компьютере с соответствующей защитой и межсетевым экраном.

Мы произвели настройку песочницы на отдельно развернутом сервере. Мы развернули сервер Jobe на основе собственных вычислительных ресурсах, следуя инструкциям на https://github.com/trampgeek/jobe. Затем мы использовали интерфейс администратора Moodle для плагина CodeRunner, чтобы указать имя хоста Jobe и, также номер порта. Хотя CodeRunner имеет гибкую архитектуру, которая поддерживает различные способы выполнения задач обучающегося в защищенной среде (песочнице). В этой изолированной программной среде используется отдельный сервер, разработанный специально для использования CodeRunner, который в спецификации называется Jobe . Основные этапы настройки отражены на рисунках 10- 16.
На рисунке 10 - интерфейс программы PuTTY, с помощью нее подключаемся к серверу 46.36.218.199 по SSH.

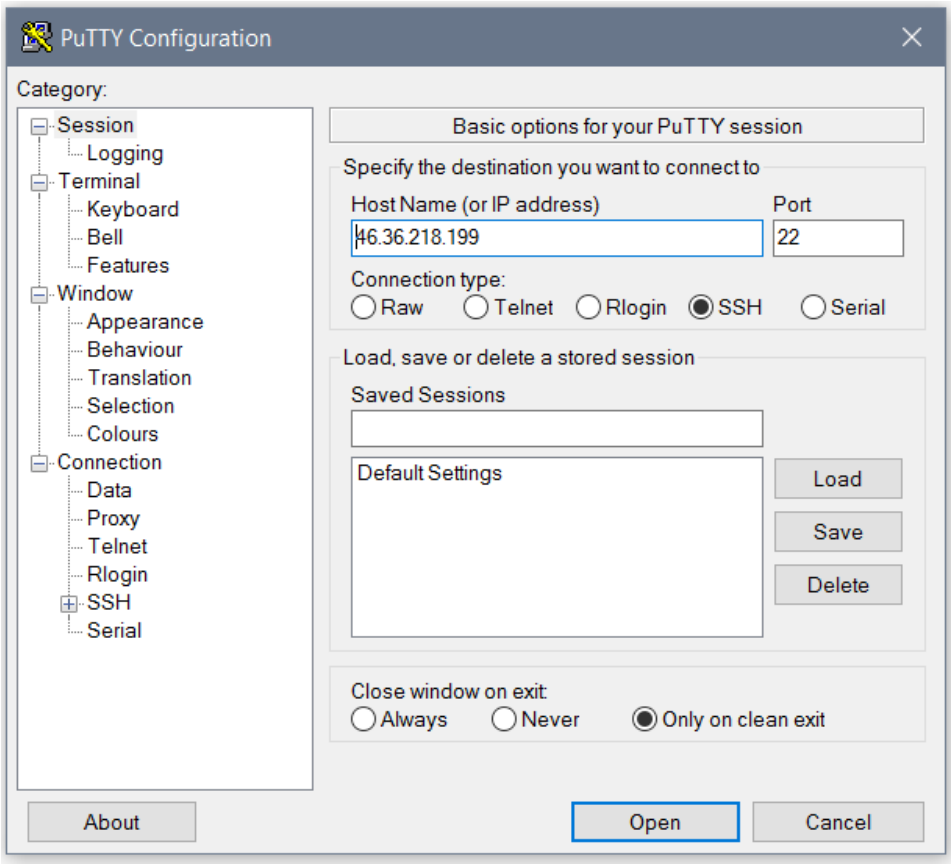

Рисунок 7

На рисунке 8 скриншот общий вид сервера

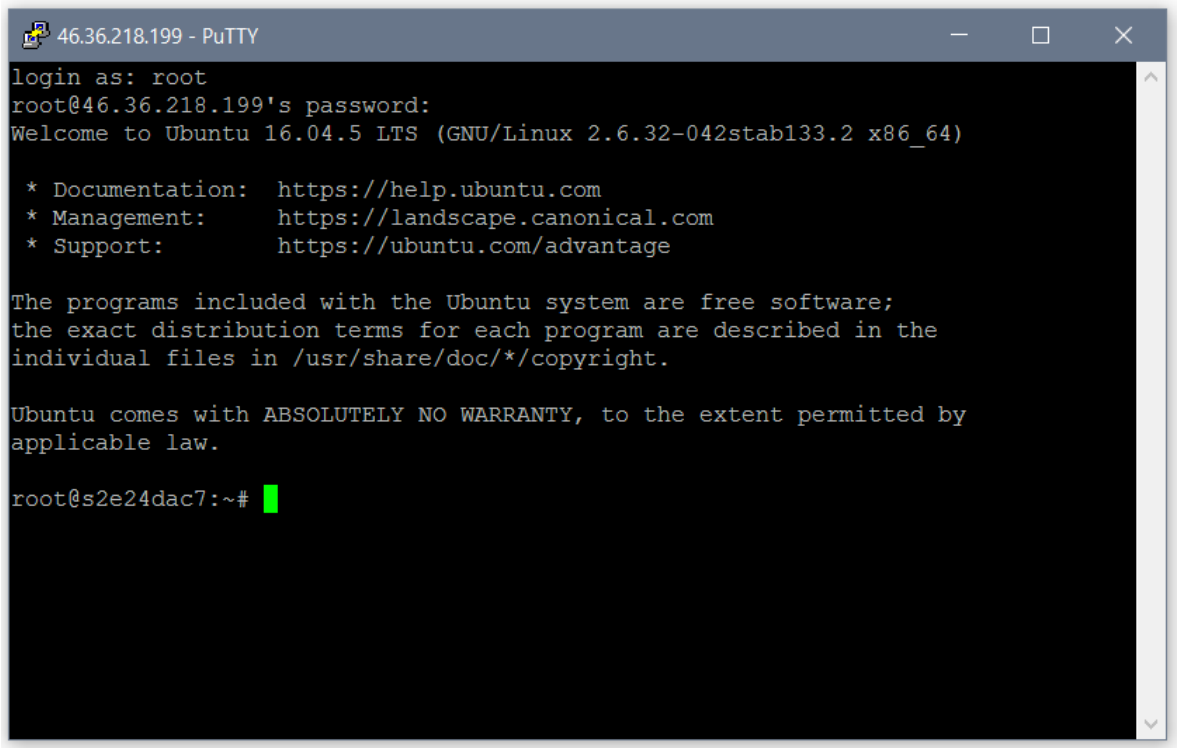

Рисунок 8

Перед тем как приступить к установке и настройке нашей песочницы необходимо обновить нашу операционную систему и список пакетов, чтобы иметь под рукой самые последние обновления безопасности. Этой командой обновляем список пакетов – рисунок 9

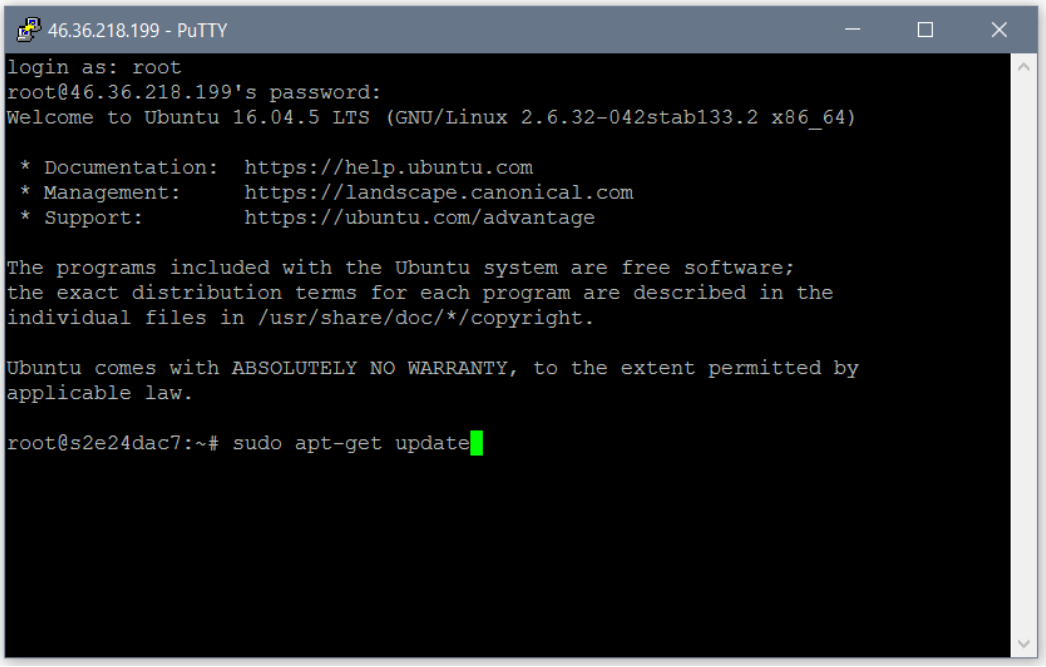

Рисунок 9

После того как мы получили список пакетов, обновляем систему – рисунок -10.

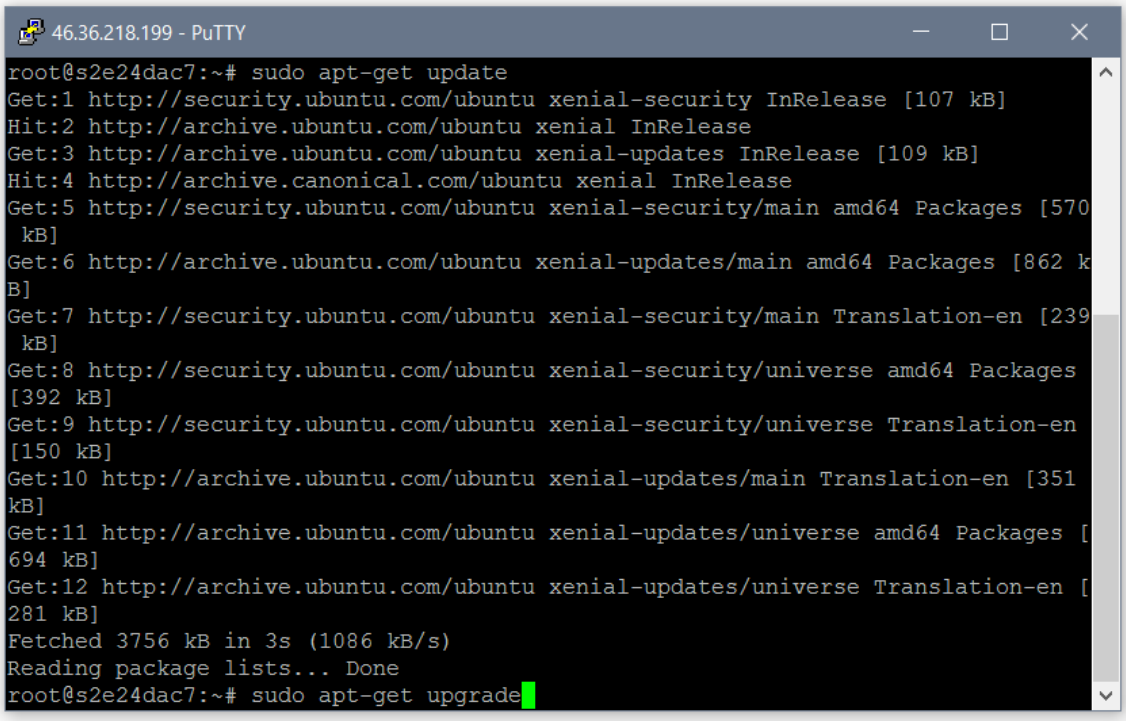

Рисунок 10

Соглашаемся и устанавливаем необходимые пакеты – рисунок 11

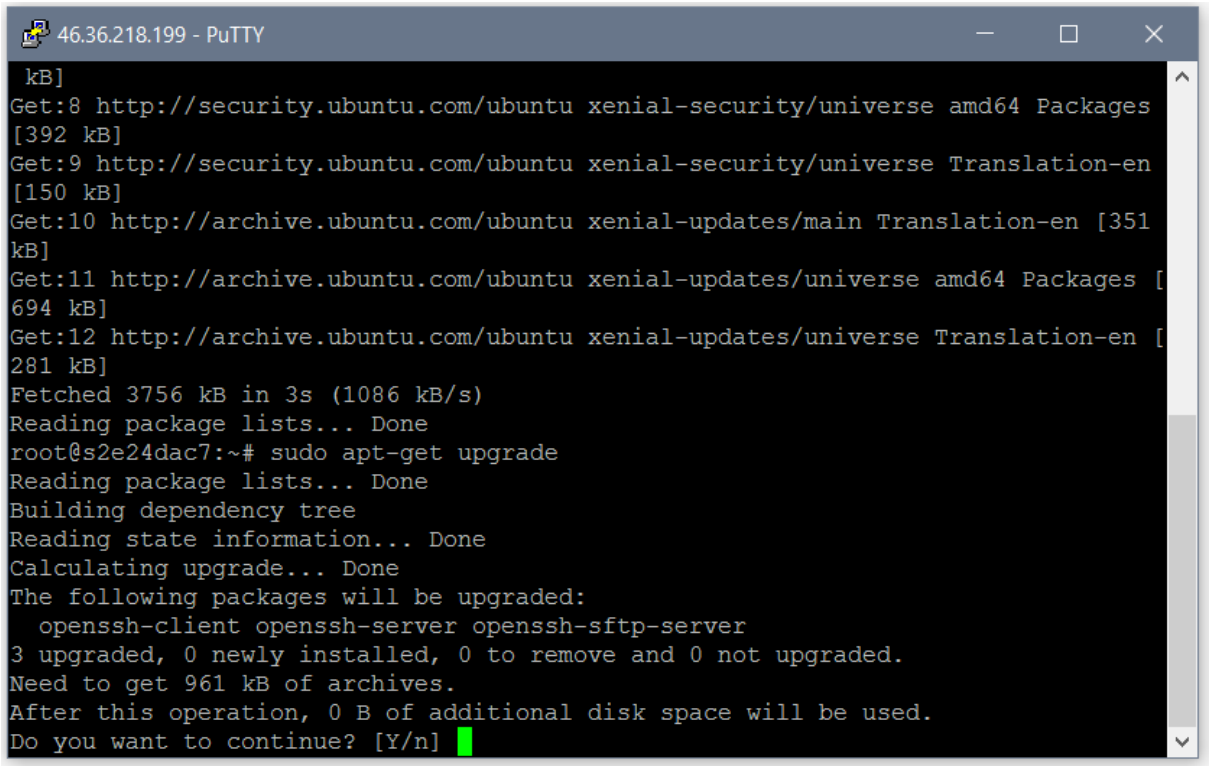

Рисунок 11

Следующей командой устанавливаем все вспомогательное программное обеспечение, которое нам понадобится для работы песочницы – рисунок 12.

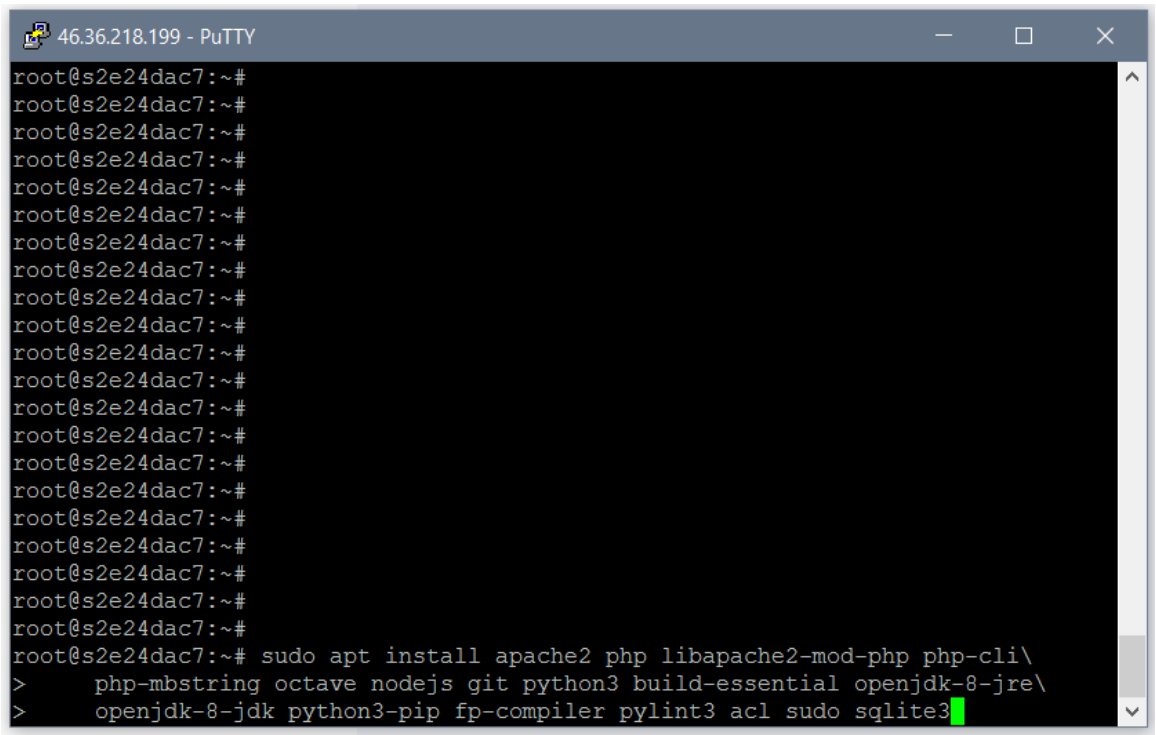

Рисунок 12

Установка вспомогательных пакетов закончена – рисунок 13

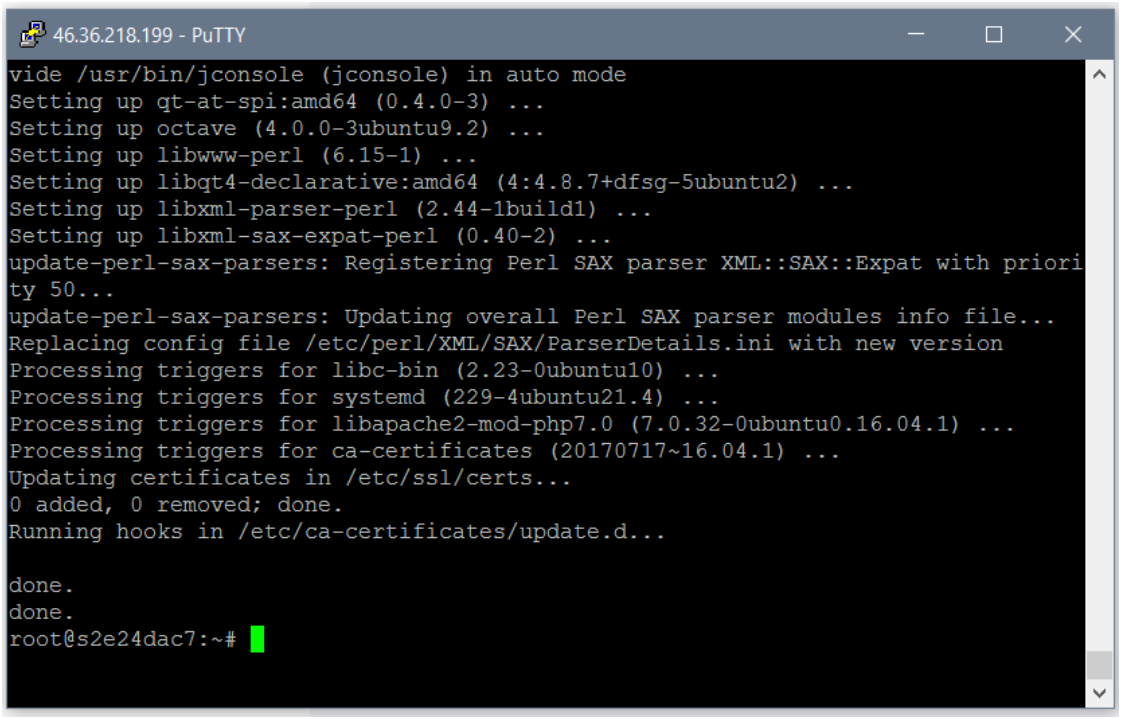

Рисунок 13

Переходим в корневой каталог веб-сервера и клонируем установочные файлы самой песочницы с репозитория GIT – рисунок 14.

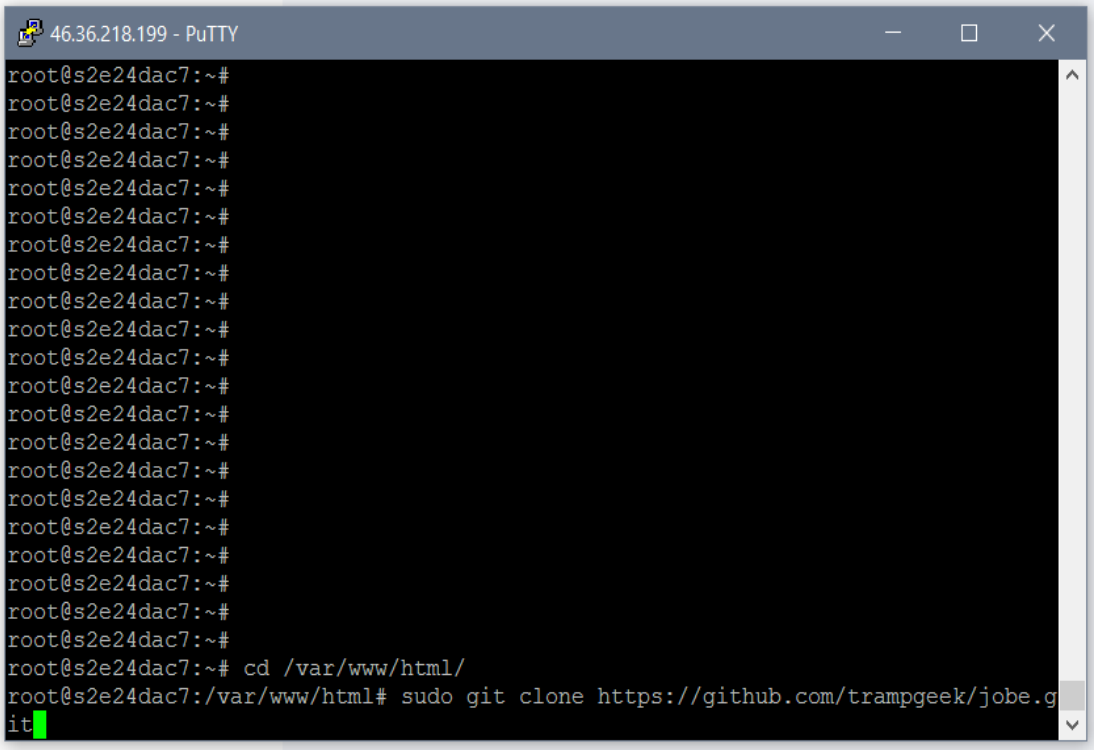

Рисунок 14

Клонирование репозитория завершено – рисунок 15.

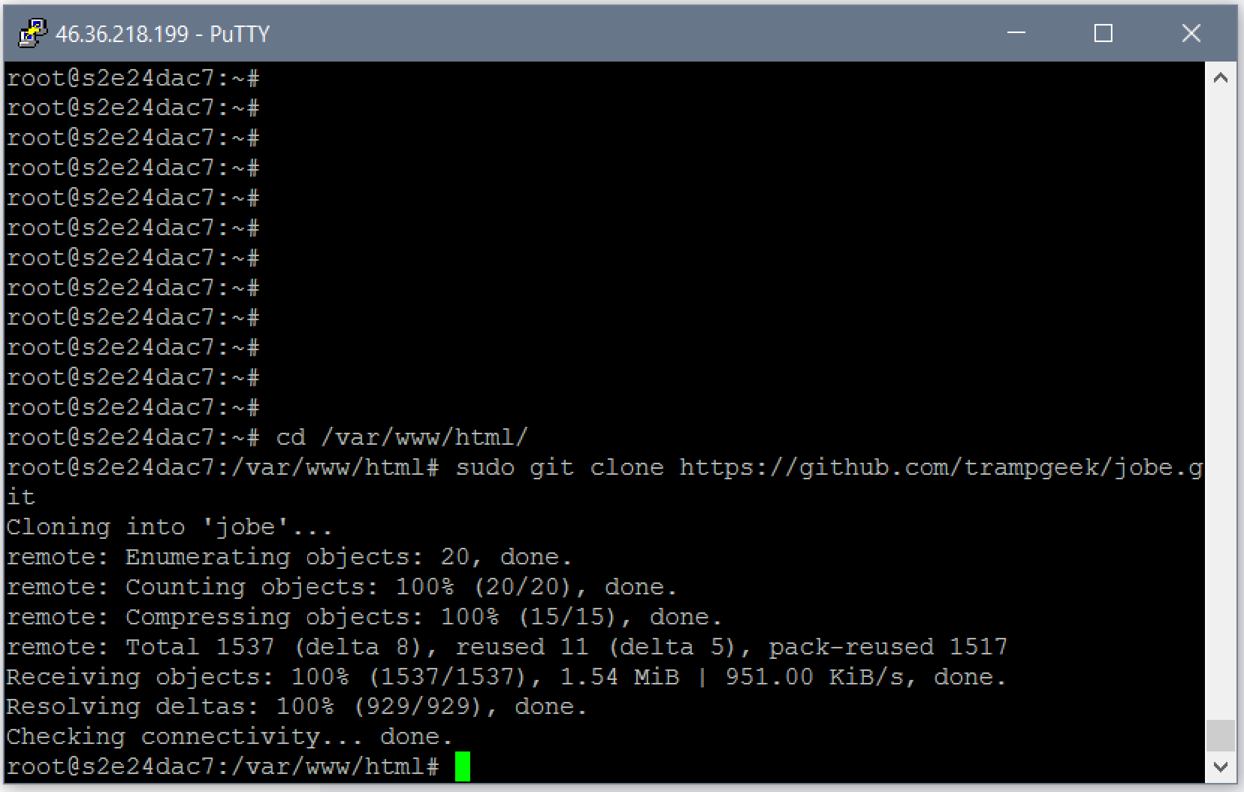

Рисунок 15

Переходим в каталог песочницы и запускаем установку – рисунок 16.

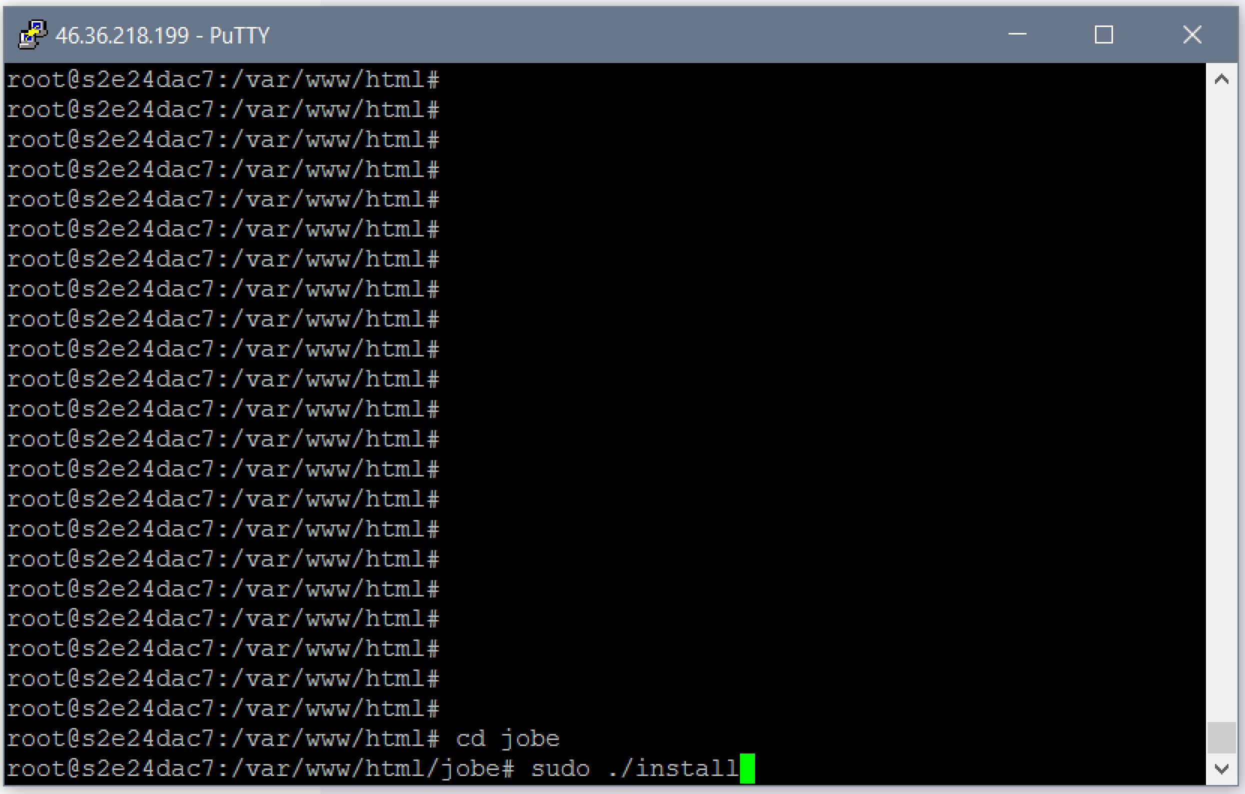

Рисунок 16

Установка песочницы завершена - рисунок 17.

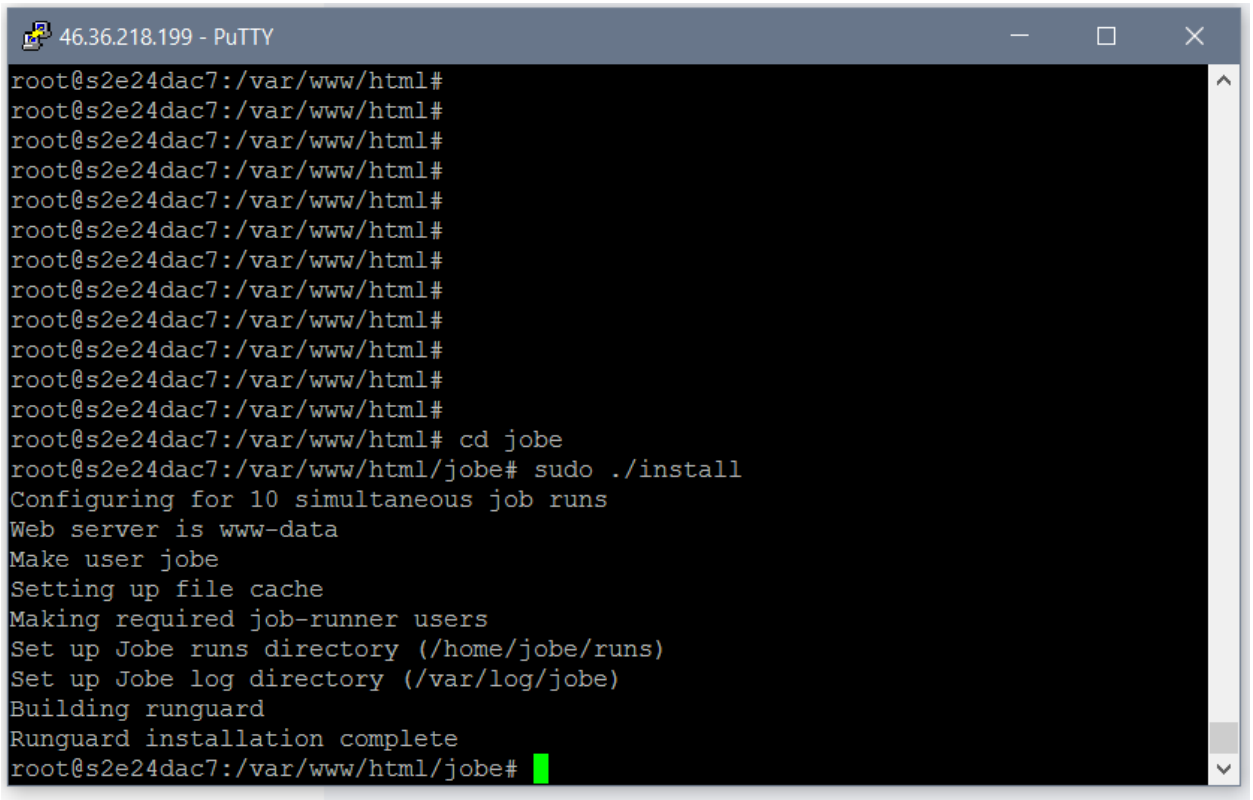

Рисунок 17

В текстовом редакторе nano открываем конфигурационный файл Apache, нам необходимо изменить локаль по умолчанию – рисунок 18.

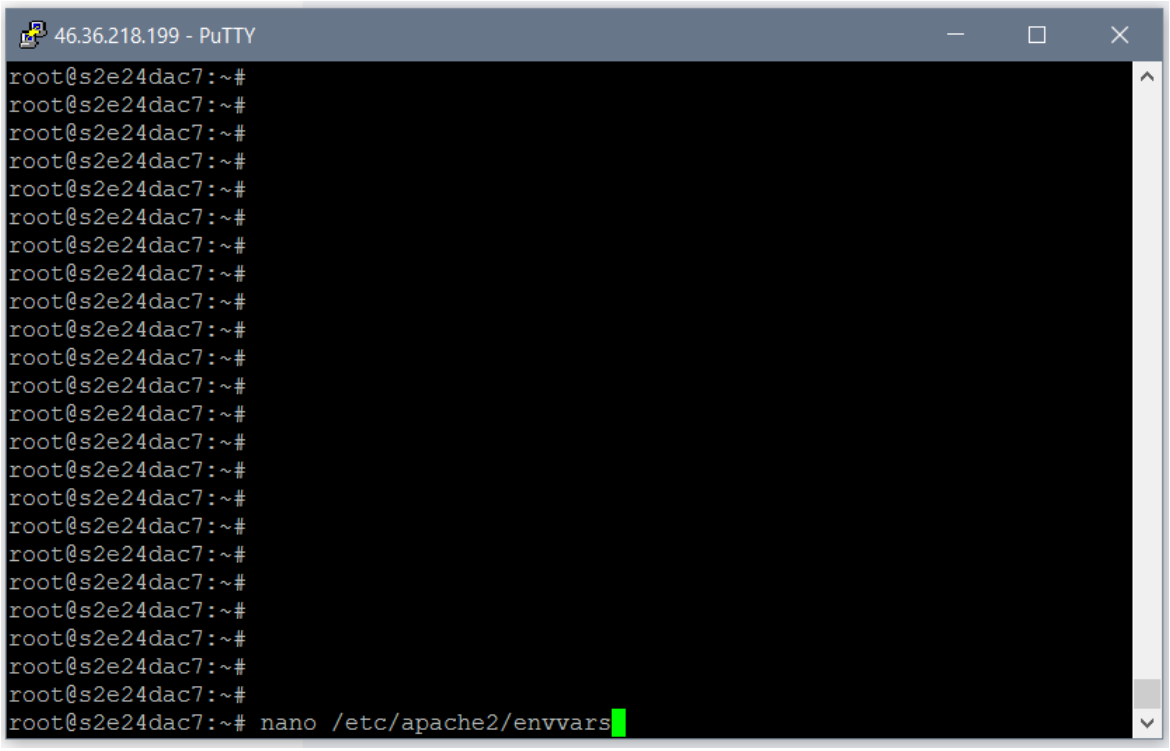

Рисунок 18

Меняем выделенную строку на export LANG=C.UTF-8 и сохраняем изменения в файле – рисунок 19.

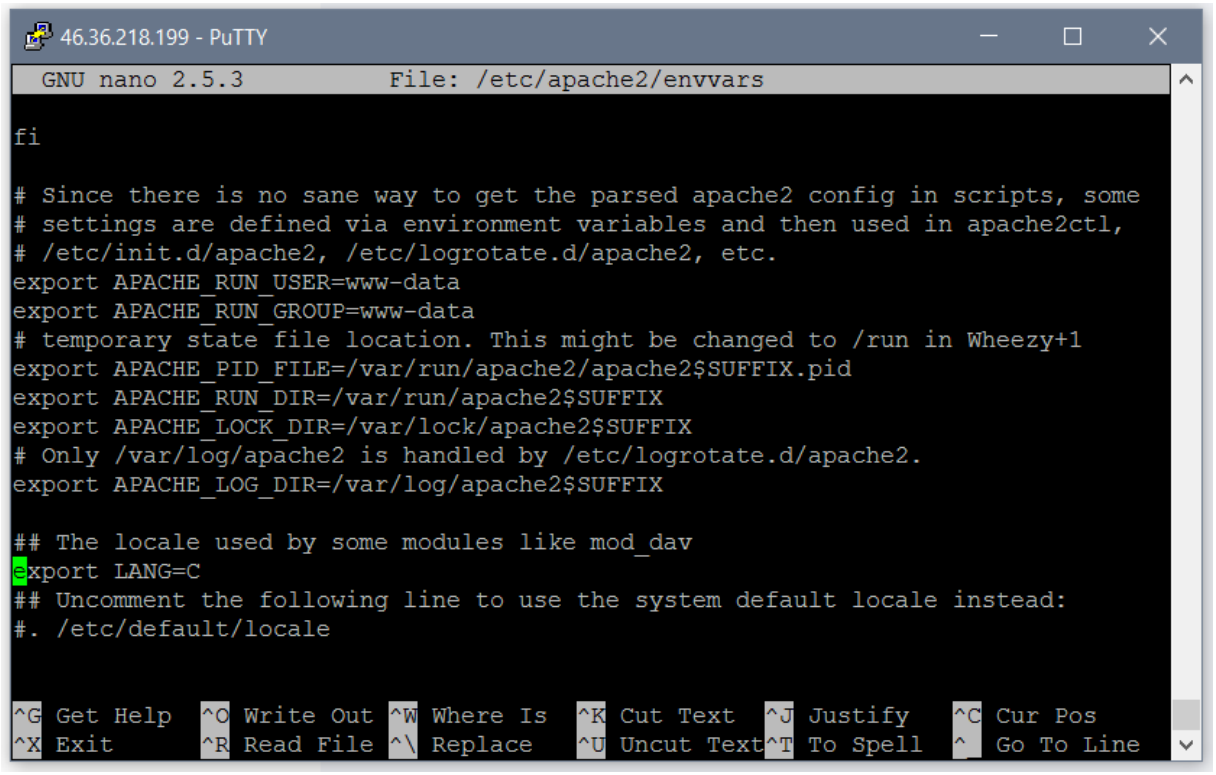

Рисунок 19

Перезагружаем службу Apache чтобы все изменения применились – рисунок 20.

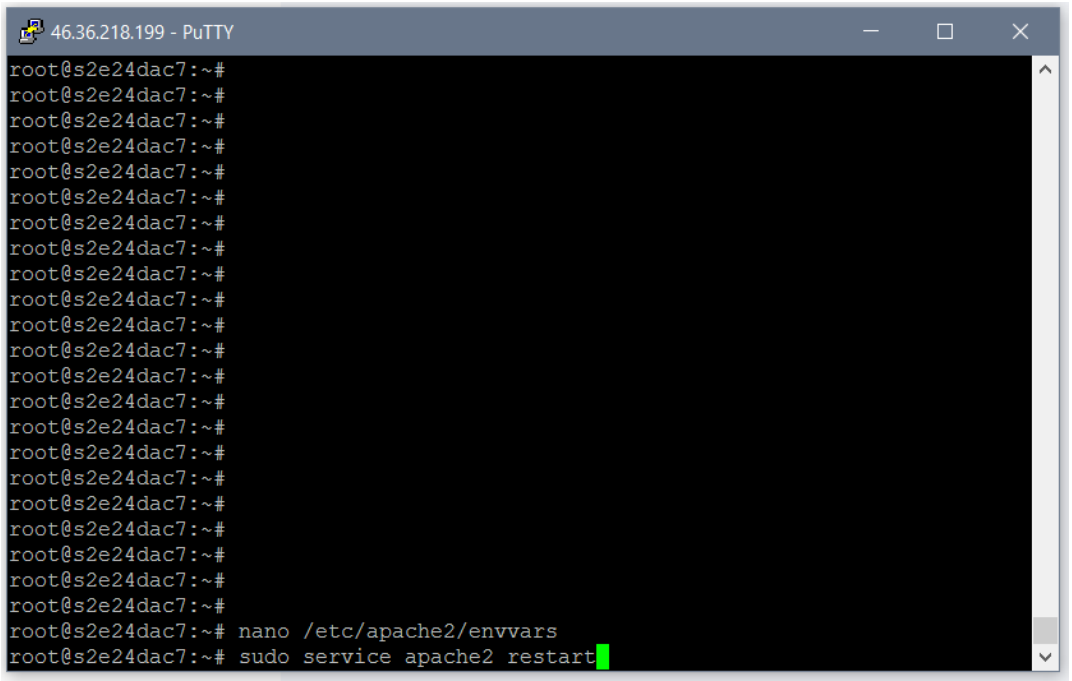

Рисунок 20

Тестируем нашу песочницу запуская тест testsubmit.py – рисунок 21

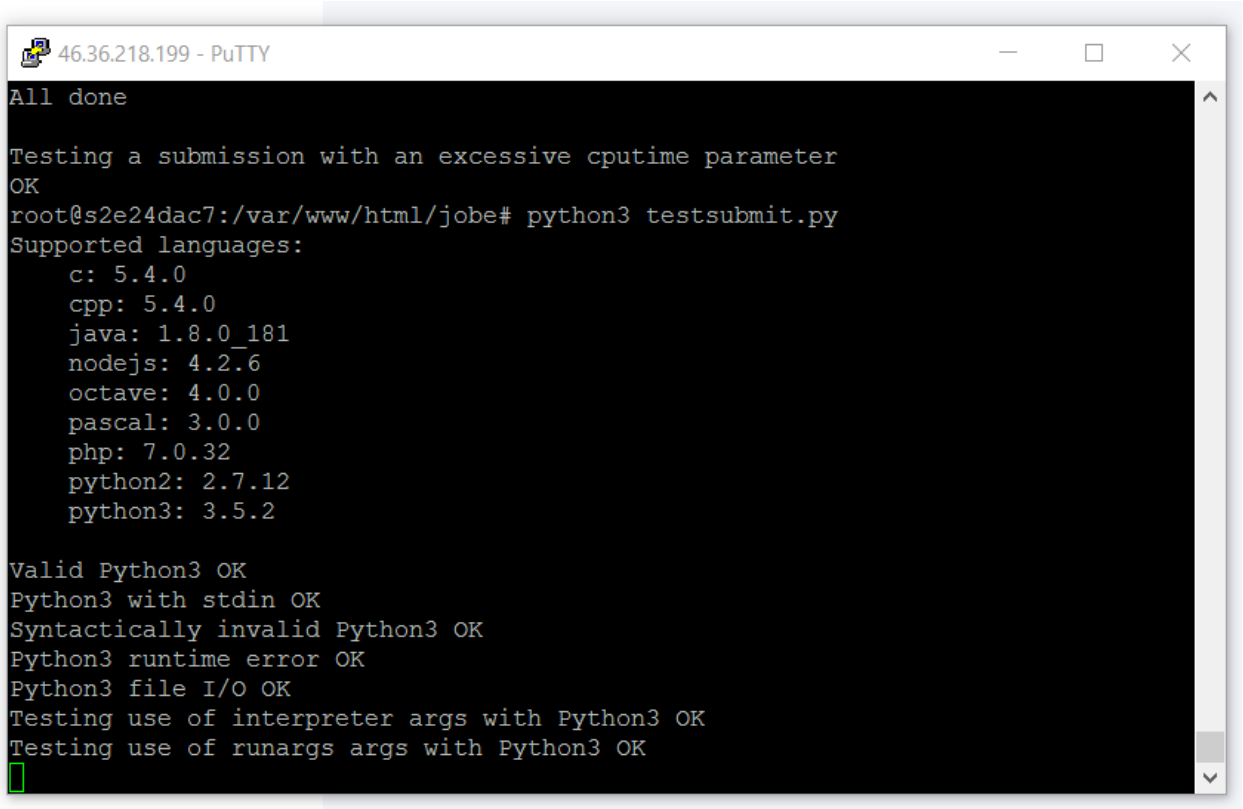

Рисунок 21

Тестирование всех параметров прошло успешно, песочница функционирует – рисунок 22.

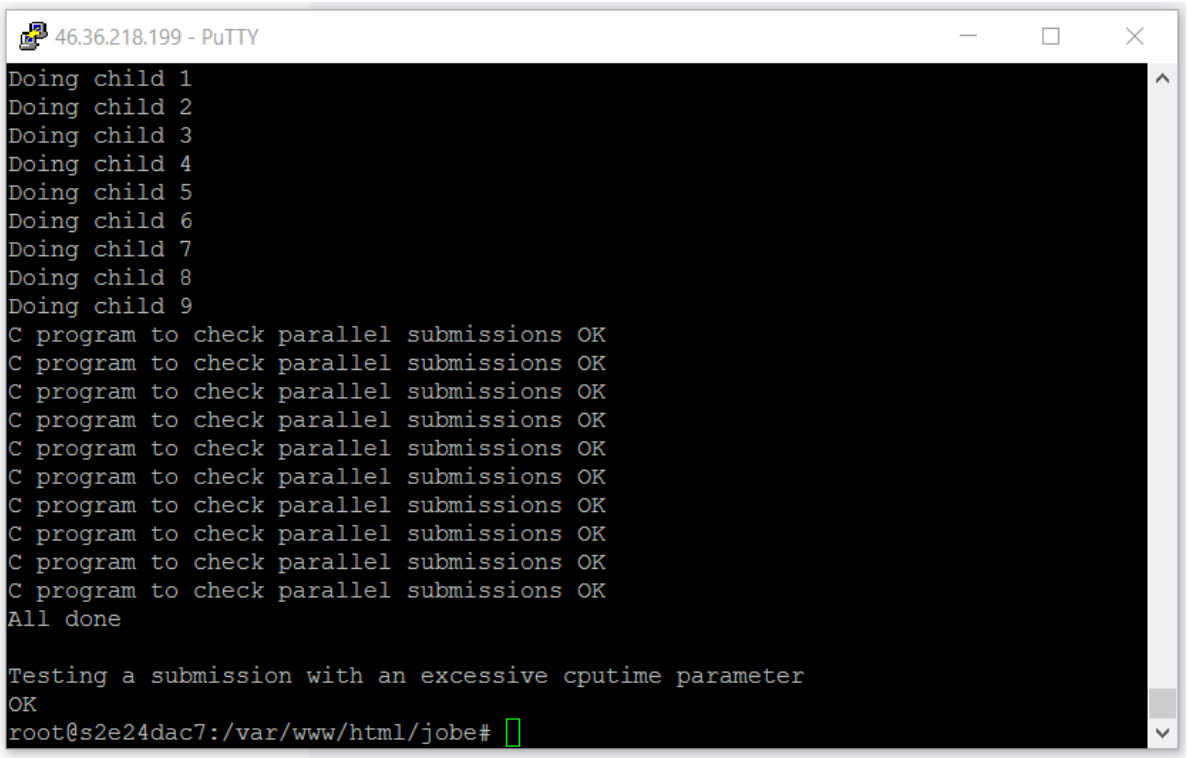

Рисунок 22

Поскольку мы создали Jobe на отдельном сервере, JobeSandbox полностью изолирует код отдельного пользователя (студента) от сервера Moodle. Существует малая вероятность того, что некий злонамеренный программный код может отключить сервер песочницы и появится возможность нарушения безопасности на сервере Moodle, например, для взлома базы данных Moodle. Однако, Moodle ведет подробный журнал всех событий, поэтому студент, сознательно нарушающий безопасность, принимает на себя риск быть уличенным нарушителем.

CodeRunner требует двух отдельных плагинов, один предназначен для конкрентых типов вопросов, а другой - для специализированного адаптивного поведения. Плагины находятся в двух разных репозиториях github: github.com/trampgeek/moodle-qbehaviour_adaptive_adapted_for_coderunner и github.com/trampgeek/moodle-qtype_coderunner.

Синтаксис Twig {{STUDENT_ANSWER | e ('py')}} приводит к тому, что представление студента фильтруется с помощью функции escape, соответствующей языку Python, которая экранирует все символы двойной кавычки и обратной косой черты с добавленной обратной косой чертой. Любой вывод, записанный в *stderr* , интерпретируется CodeRunner как ошибка времени выполнения, которая прерывает последовательность тестов, поэтому студент видит вывод ошибок только в первом тестовом примере.

Мы произвели настройку таблицы результатов следующим образом. Выходные данные стандартных грейдеров представляют собой список так называемых объектов *TestResult* , каждый из которых имеет следующие поля (которые включают в себя фактические данные тестового примера):

```
testcode      // The test that was run (trimmed, snipped)
iscorrect     // True iff test passed fully (100%)
expected      // Expected output (trimmed, snipped)
mark          // The max mark awardable for this test
awarded       // The mark actually awarded.
```

got // What the student's code gave (trimmed, snipped)

stdin // The standard input data (trimmed, snipped)

extra // Extra data for use by some templates

Поле с именем *result_columns* в форме создания вопроса было использовано нами в таблице результатов.

Каждый спецификатор столбца сам по себе является списком, обычно с двумя или тремя элементами. Первый элемент - это заголовок столбца, второй элемент - это обычно поле из объекта TestResult, отображаемого в столбце (одно из значений, перечисленных выше), а необязательный третий элемент - это sprintf строка формата, используемая для отображения поля. Грейдеры шаблонов для каждого теста могут добавлять свои собственные поля, которые также могут быть выбраны для отображения. Также возможно объединить несколько полей в столбец, добавив дополнительные поля к спецификатору: они должны предшествовать sprintf спецификатору формата, который затем становится обязательным. Например, для отображения Mark Fraction столбца в форме можно использовать 0.74 out of 1.00 спецификатор формата столбца ["Mark Fraction", "awarded", "mark", "%.2f out of %.2f"].

В качестве особого случая формат %hозначает, что поле результата теста должно быть взято как готовый к выводу HTML и не должно подвергаться дальнейшей обработке; это может быть полезно для шаблонов пользовательских грейдеров, которые генерируют вывод HTML, таких как графика SVG, и мы также использовали его в вопросах, где вывод из программы студента был HTML.

Мы сделали небольшое упрощение. Синтаксис фактически допускает выражения в форме:

filter(testResultField [,testResultField]...)

где filter- имя встроенной функции фильтра, которая каким-либо образом фильтрует заданное поле (поля) testResult. На данный момент единственной такой встроенной функцией фильтра является diff. Это (или

было) функция, принимающая два поля результатов теста в качестве параметров и возвращающая строку HTML, представляющую первое поле теста со встроенными элементами HTML <ins> и <del>, которые показывают вставки и удаления, необходимые для преобразования первого поля во второй. Это было использовано для обеспечения поддержки кнопки.

Показ различий автоматически отображается, если ответ помечен как неправильный, и если используется грейдер с точным соответствием. Следовательно, функция *diff* фильтра больше не функционирует, но остается синтаксически поддерживаемой для поддержки устаревших вопросов, которые ее используют.

Начиная с версии 3.3.0, CodeRunner поддерживает подключаемые пользовательские интерфейсы, хотя администратор должен установить плагин. В настоящее время в CodeRunner встроены два пользовательских интерфейса: Ace и Graph. Мы выбрали необходимый пользовательский интерфейс через раскрывающееся меню в разделе настроек формы автора вопроса. Выбор управляет редактированием полей предварительного ответа и предварительного ответа формы авторинга и ответа учащегося в реальном тесте. Редактор Ace всегда используется для редактирования самого шаблона, если только он не отключен с помощью *шаблона,* в поле создания *используется* флажок *ace* .

Плагин Graph UI, который на данный момент следует рассматривать как экспериментальный, предоставляет простые возможности рисования графиков для поддержки вопросов, когда ученика просят нарисовать или отредактировать график. По умолчанию пользовательский интерфейс Graph, разработанный для конечных автоматов, рисует ориентированные графы, позволяет узлам помечаться как состояния *Accept* и позволяет входящим начальным ребрам. Например:

В текущих настройках доступны три служебных скрипта, связанных с CodeRunner. Первоначально предназначенные только для использования администратором, они оказываются полезными и для преподавателей. В

развертываемой нами изолированной среде функционал этих скрпитов сохранен.

Три сценария:

1. <moodle_home> /question/type/coderunner/bulktestindex.php Этот сценарий отображает список всех категорий вопросов, доступных пользователю, который в данный момент вошел в Moodle на компьютере, на котором выполняется сценарий. Каждая категория отображается в виде интерактивной ссылки, которая затем запускает сценарий, который проверяет примеры ответов на все вопросы в этой категории, сообщая обо всех успехах и неудачах.

2. <moodle_home> /question/type/coderunner/prototypeusageindex.php В этих сценариях отображается индекс, подобный приведенному выше, за исключением того, что теперь по интерактивным ссылкам теперь запускается сценарий, который сообщает об использовании прототипа вопроса в этой категории.

3. <moodle_home> /question/type/coderunner/downloadquizattempts.php Этот сценарий, который все еще является экспериментальным, отображает список всех тестов, доступных для вошедшего в систему пользователя, что позволяет им загружать электронную таблицу всех представлений в выбранный тест всех обучающихся. Загруженная электронная таблица подходит для автономного анализа и содержит информацию, отсутствующую в экспортированном файле ответов Moodle, такую как все промежуточные подпункты и предварительные проверки и время каждого такого действия.

Загрузка может быть в формате CSV или Excel; последнее рекомендуется для большинства случаев, потому что давняя ошибка в fputcsvфункции PHP может привести к повреждению выходных

файлов csv. Экспортированная электронная таблица Excel может быть открыта в Excel или Open Office и сохранена как CSV.

Формат загрузки требует хорошего понимания схемы базы данных Moodle. Используется следующий запрос, где каждая строка результата выводится как одна строка электронной таблицы.

```
SELECT
    concat(quiza.uniqueid, qasd.attemptstepid, qasd.id) as uniquekey,
    quiza.uniqueid as quizattemptid,
    timestart,
    timefinish,
    u.firstname,
    u.lastname,
    u.email,
    qatt.slot,
    qatt.questionid,
    quest.name as qname,
    slot.maxmark as mark,
    qattsteps.timecreated as timestamp,
    FROM_UNIXTIME(qattsteps.timecreated,'%Y/%m/%d
%H:%i:%s') as datetime,
    qattsteps.fraction,
    qattsteps.state,
    qasd.attemptstepid,
    qasd.name as qasdname,
    qasd.value as value
FROM {user} u
JOIN {quiz_attempts} quiza ON quiza.userid = u.id AND quiza.quiz
= :quizid
JOIN {question_attempts} qatt ON qatt.questionusageid =
quiza.uniqueid
```

JOIN {question_attempt_steps} qattsteps ON qattsteps.questionattemptid = qatt.id

JOIN {question_attempt_step_data} qasd on qasd.attemptstepid = qattsteps.id

JOIN {question} quest ON quest.id = qatt.questionid

JOIN {quiz_slots} slot ON qatt.slot = slot.slot AND slot.quizid = quiza.quiz

WHERE quiza.preview = 0

AND (qasd.name NOT RLIKE '^-_' OR qasd.name = '-_rawfraction')

AND qasd.name NOT RLIKE '^_'

AND quest.length > 0

ORDER BY quiza.uniqueid, timestamp;

Этот запрос приводит к появлению нескольких почти идентичных строк для одного действия студента (например, отправка ответа) с разными парами (qasdname, value). ['qasdname' является name столбцом таблицы вопрос-попытка-шаг-данных и value является значением, связанным с этим именем. Набор таких пар (ключ, значение) зависит от типа вопроса и конкретного записываемого действия пользователя.] В настоящее время так называемые «переменные поведения» - те, которые содержат подчеркивание - не включаются в экспорт, за исключением переменной -_rawfraction. Это должно ограничить объем данных, но оптимизация нами не проверялась.

Обработка исходной электронной таблицы опирается на файл, quizsubmissions.рувключенный в репозиторий git, определяет классы Python для упрощения процесса. Заявления

from quizsubmissions import QuizSubmissions

submission_data = QuizSubmissions(csvfilename)

позволяют импортировать экспортированную электронную таблицу и дает легкий доступ к данным о каком-либо конкретном

пользователе системы (студенте) и фиксации их действий при доступе к информационным ресурсам, размещенным в песочнице.

Доступно много другой статистической информации, такой как имя студента, все промежуточные материалы и предварительные проверки, их время и т.д. Она хранится в служебном файле и может быть импортирована в раздел, который будет доступен для просмотра преподавателями.

Таким образом нами была произведена настройка песочницы как частный случай реализации технологии виртуализации на собственных ресурсах – развернутом сервере, но ассоциированном с корпоративной сетью ГПБОУ «ЮУрГТК».

3.2.Настройка сетевых правил для предотвращения несанкционированного доступа

Отправленные пакеты в песочницу или из нее, как правило, могут записывать файлы только во временный каталог, созданный для их запуска в каталоге / home / jobe / run. Исключениями из этого правила являются каталоги / tmp, / var / tmp, / var / crash и / run / lock, которые обычно могут быть записаны любым процессом ОС.

Временный рабочий каталог и любые файлы в записываемых каталогах, упомянутых выше, удаляются по окончании прогона. Однако, в зависимости от размера различных разделов и максимально допустимого времени выполнения, для преднамеренного злоумышленника в принципе может быть достаточно запустить систему из дискового пространства в определенном разделе (вероятно, / tmp, который обычно относительно небольшой), прежде чем работа заканчивается. Это, в свою очередь, может повлиять на другие выполняемые работы

. При стандартном времени выполнения, составляющем несколько секунд, задания задерживаются задолго до того, как они могут заполнить основной раздел. Заполнение / tmp проще, но задания обычно не должны

использовать этот каталог, поэтому злоумышленный процесс, который заполняет его, не должен влиять на других пользователей. В любом случае пространство освобождается, как только работа заканчивается.

Возможность защиты от такого исхода реализуется путем установки дисковых квот для пользователей jobe00, jobe01, ... jobe09 .Количество таких учетных записей пользователей определяется параметром jobe_max_usersв application/config/config.php, Значение по умолчанию - 10.

По умолчанию ожидается, что Jobe будет работать на сервере интрасети, который защищен брандмауэром и разрешает доступ только с определенных авторизованных хостов. В этом режиме предполагается, что клиент является доверенным, и ему не нужно предоставлять какую-либо форму авторизации или аутентификации. Также важно запретить серверу Jobe открывать соединения с другими компьютерами, чтобы программа учащегося не могла выполнять такие неприятные действия, как сканирование портов в вашей внутренней сети.

Использование ufw (Uncomplicated Firewall) - возможная последовательность команд, которая ограничит исходящий трафик только одним назначенным хостом («некоторый полезный ip») на портах 80 и 443, разрешит доступ по ssh (порт 22) из любого места и веб-доступ к jobe (предполагается) находиться на порте 80) только от одного указанного клиента:

```
ufw default reject outgoing
ufw allow out proto tcp to <some_useful_ip> port 80,443
ufw allow in 22/tcp
ufw allow in proto tcp to any port 80 from <your_client_ip>
ufw enable
```

Рисунок 23

Выше <your_client_ip> - это хост, которому разрешено отправлять задания в Jobe (например, сервер Moodle с CodeRunner). <some_useful_ip> -

это любой сервер, к которому Jobe может понадобиться подключиться для запуска / оценки кода студента. При отсутствии такого сервера эта строка должна быть пропущена.

Когда Jobe обслуживает несколько клиентов/процессов, необходимо настроить брандмауэр так, чтобы разрешать входящие подключения из любого места, но затем вам также следует настроить сервер остальных серверов, чтобы требовать некоторую форму проверки подлинности и авторизации. Различные способы достижения этого возможны при использовании плагина rest-server.

Самый простой подход к авторизации - предоставить ключ API для каждого запроса. Затем клиент должен предоставить ключ с каждым запросом в заголовке X-API-Key формы:

```
X-API-KEY: <key>
```

Чтобы настроить Jobe для работы таким образом, мы произвели следующие действия:

1. Были установлены дополнительные зависимости для аутентификации по API-ключу.
2. Создана база данных с именем *jobe* и были определены пользователи с полным доступом к ней. (В реальном образовательном процессе она может быть расширена).
3. Отредактирован файл *application / config / database.php,* для получения доступа к серверу mysql и базе данных jobe с учетными данными пользователя, которые мы определили на предыдущем шаге.
4. Отредактирован файл *application / config / rest.php* и установлен для параметра конфигурации *rest_enable_keys*значение 1.
5. Настроена таблица keysи limitskак с несколькими ключами API, которые затем используются при любых запросов к серверу Jobe.

При обслуживании нескольких клиентов имеется возможность ограничить использование сервера одним или несколькими клиентами. Это можно сделать, установив параметр *rest_enable_limits* в *application / config /*

rest.php на ненулевое значение. Затем Jobe ограничит количество запросов, сделанных с любым данным ключом, значениями, установленными в *application / config / per_method_limits.php* .

Чтобы это работало, *база* данных *jobe* должна содержать дополнительные *ограничения* таблицы , определенные командой SQL, например таким образом:

```
CREATE TABLE `limits` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `uri` varchar(255) NOT NULL,
  `count` int(10) NOT NULL,
  `hour_started` int(11) NOT NULL,
  `api_key` varchar(40) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Рисунок 24

Документ спецификации Jobe REST API определяет формат так называемой *run_spec* , которая представляет собой запись / объект, которая закодирована в запросе POST или запросе запуска для указания сведений о задании. Он включает language_id, исходный код, имя исходного файла, любые стандартные входные данные, список необходимых файлов и набор параметров задания. Параметры задания не определяются API REST, так как они зависят от реализации. Этот раздел определяет формат *параметры* поля *run_spec* в этой реализации.

Допустимые атрибуты поля параметров, а также их глобальные значения по умолчанию в скобках:

1. disklimit (20): максимальное количество мегабайт, которое может быть записано в файл (ы) диска перед отменой задания
2. streamsize (2): максимальное количество мегабайт стандартного вывода до прерывания задания.

3. cputime (5): максимальное количество секунд процессорного времени до отмены задания

4. memorylimit (200): максимальное количество мегабайт памяти, которое может использовать задача. Это значение используется для установки Linux RLIMIT_STACK, RLIMIT_DATA и RLIMIT_AS через системный вызов *setrlimit* . Если значение превышено, задание не прерывается, но вызовы malloc и / или mmap не смогут выделить больше памяти с несколько непредсказуемыми результатами, хотя ошибка сегментации является наиболее вероятным результатом.

5. numprocs (20): максимальное количество процессов, которое разрешено заданием. Если это будет превышено, системный вызов *fork* завершится неудачей, опять же с несколько непредсказуемыми результатами.

6. compileargs ([]): список значений строковых опций для передачи компилятору, например, ["-Wall", "-std = c99"] для компилятора Си. Имеет смысл только для скомпилированных языков. Эти аргументы предшествуют имени файла для компиляции.

7. linkargs ([]): список значений строковых опций, передаваемых компилятору, например ["-lm"] для компилятора Си. Эти аргументы следуют за именем файла для компиляции. Имеет смысл только для некоторых скомпилированных языков, особенно C и C ++.

8. interpreterargs ([]): список значений строковых опций, передаваемых интерпретатору языка или Java VM и т. д. при выполнении программы. Имеет смысл только для таких языков, как Python, PHP и Java, где выходные данные компилятора не являются чисто исполняемым машинным кодом.

9. runargs ([]): список значений строковых опций для передачи в исполняемую программу, например, для установки *argc* и *argv* для C-

программы. Обычно не используется в CodeRunner, поскольку нет возможности устанавливать параметры для каждого теста.

Если какой-либо из вышеперечисленных атрибутов определен в поле *параметров* run_spec , используется последний, а значения по умолчанию игнорируются.

Версия Jobe была настроена для использования Moodle Coderunner. При использовании Jobe из CodeRunner различные параметры компиляции и запуска языка можно изменить с помощью поля параметров песочницы.

Таким образом мы произвели настройку сетевых правил, описанных выше.

3.2. Экспериментальная проверка мер и анализ полученных данных

Современные системы обнаружения нарушения информационной безопасности включают в себя системы виртуализации, песочницы со встроенными системами управления знаниями о киберугрозах и уязвимостях (Threat Intelligence) [46].

Многие ведущие производители систем информационной безопасности внедрили песочницы в свои продукты как средство проактивной защиты, помимо этого появились специализированные программы, позволяющие запускать приложения в изолированной среде исполнения. Как правило, песочницы используют для запуска непроверенного кода из неизвестных источников как средство проактивной защиты от сетевых атак, а также для обнаружения и анализа вредоносных программ. Также зачастую песочницы используются в процессе разработки программного обеспечения для запуска «сырого» кода, который может случайно повредить систему или испортить сложную конфигурацию. Такие песочницы копируют основные элементы среды, для которой пишется код, и позволяют разработчикам быстро и безболезненно экспериментировать с неотлаженным кодом.

При настройке песочницы на отдельно выделенном сервере при разработке многопользовательского тренажера для ГБПОУ «ЮУрГТК» мы использовали изоляцию на основе полной виртуализации. Использование любой виртуальной машины в качестве защитного слоя над гостевой операционной системой, где установлен браузер и иные потенциально опасные программы, через которые пользователь может заразиться, дает достаточно высокий уровень защиты основной рабочей системы. Попытка модификации каких-либо объектов приведет к изменению лишь их копий внутри песочницы, реальные данные не пострадают. Контроль прав не дает возможности атаковать основную систему изнутри песочницы через интерфейсы операционной системы. Кроме того, в качестве дополнительной защиты нами была проведена апробация сетевых правил, описанных в п.3.2.

Для выяснения степени изолированности созданной нами песочницы мы применили методику [24,25], в основе которой лежит специально разработанный программный продукт, который последовательно выполняет различные действия, напоминающие злонамеренные сетевые атаки в изолированной среде. После завершения работы вне изолированной среды можно проследить степень изоляции песочницы. В набор действий входило два десятка различных манипуляций, в том числе:

- Открытие TCP-порт для входящих соединений;

– Снятие снимка экрана;

– Запуск окна браузера за пределами;

При имитации злонамеренных сетевых атак в тестовую зону применялись методы, затрудняющие обнаружение традиционными сигнатурными средствами защиты, а именно - архивация файла с использованием форматов RAR, ZIP, 7-ZIP, в том числе с защитой архива паролем; почтовые сообщения с веб-ссылками, в том числе с использованием «коротких» URL (URL shortening); шифрование (AES) кода (payload) в макросах в документах Microsoft Word. Необходимо отметить, что поскольку все решения тестировались в реальной сети - в изолированной сетевой среде, то прежде чем попасть на анализ в песочницу, файлы со зловредным кодом проходили анализ и блокировались имеющимися у заказчика (колледжа)

средствами защиты, с использованием существующих сигнатурных и репутационных механизмов.

Результаты теста песочниц показал, что из 32 симуляций сетевых атак, используемых при тестировании анализа веб-трафика, на анализ в песочницу попало 22 события, не обнаруженных существующими сигнатурными средствами защиты. Подробная таблица по количеству выявленных в песочнице злонамеренных сетевых атак приведена в таблице 10.

Таблица10

Обнаруженные сетевые атаки: виды и количество

Тип атаки	Количество обнаружений
Mailbombing	2
IP-спуфинг	2
Man-in-the-middle	1
XSS-атака	3
XPath-инъекция	2
SQL-инъекция	2
PHP-инъекция	2
Использование уязвимости в веб-браузереWeb.Exploit	3
phishing-атаки	2
Попыток коммуникаций с внешним сервером управления ботнет-сетями (callbacks)	3

Проведенное тестирование показало высокой уровень защиты песочницы и соответственно всей информации, содержащейся в МТ по профессиональному модулю. Технология песочниц является испытанной и надежной методикой выполнения рискованных приложений и посещения потенциально опасных веб-сайтов. Проведенное исследование подтвердило выдвинутую гипотезу.

Выводы по 3 главе

Мы реализовали изолированную среду - песочницу, используя плагин CodeRunner (V3.3.0) для Moodle и специально выделенный сервер. Песочница (англ. sandbox) - это среда для безопасного исполнения компьютерных программ, представляет собой жёстко контролируемый набор ресурсов для исполнения гостевой программы. Песочницы являются реализацией виртуализации.

CodeRunner - плагин для Moodle, который позволяет организации размещать в ней электронные образовательные ресурсы.

Для повышения безопасности развернутой песочницы и организации ее функционирования нами были настроены сетевые правила для ограничения несанкционированного доступа в песочницу.

Степень изолированности песочницы мы проверяли специальной методикой, имитирующей злонамеренные сетевые атаки. При симуляции злонамеренных сетевых атак применялись методы, затрудняющие обнаружение традиционными сигнатурными средствами защиты. Поскольку все решения тестировались в реальной сети - в изолированной сетевой среде, физически - на выделенном сервере, то прежде чем попасть на анализ в песочницу, симуляции блокировались имеющимися у заказчика (колледжа) средствами защиты, с использованием сигнатурных, репутационных и других механизмов.

Результаты теста песочницы показали, что из симуляций сетевых атак используемых при тестировании степени изолированности песочницы, на анализ в песочницу попало большая их часть, где была выявлена и зафиксирована. Результаты тестирования песочницы и настроенных сетевых правил показали высокий уровень безопасности, что доказывает ранее выдвинутую гипотезу.

Заключение

В процессе проведенного исследования при подготовке магистерской диссертации нами была изучены научно-методические, нормативно-правовые и технические информационные источники, на основе которых были проанализированы содержание, структура, дидактические возможности и функциональные особенности функционала электронных образовательных ресурсов. Также мы выявили основные этапы разработки электронных образовательных ресурсов, их виды и процедуру применения в образовательном процессе современной образовательной организации СПО.

Нами был разработан электронный образовательный ресурс – практикум для формирования компетенций по профессиональному модулю, содержательно направленным на освоение языка программирования PHP/ Были также выявлены критерии оценки электронных образовательных ресурсов, используя которые мы провели экспертную оценку разработанного программного педагогического средства.

В ходе исследования нами было проанализировано состояние защищенности электронных образовательных ресурсов в ГБПОУ «ЮУрГТК», выявлены существующие уязвимости. Анализ показал, что наибольшие риски имеются при реализации угроз нелегального проникновения злоумышленников под видом санкционированных пользователей и доступа несанкционированных пользователей к сети.

Выявленные уязвимости и угрозы информационной безопасности позволили уточнить меры защиты. Нами была реализована изолированная среду – песочница (англ. sandbox) на специально выделенном сервере. Песочница представляет собой жёстко контролируемый набор ресурсов для исполнения гостевой программы и являются частной реализацией виртуализации.

Для повышения безопасности развернутой песочницы и организации ее функционирования нами были настроены сетевые правила для ограничения

несанкционированного доступа в песочницу с учетом проведенного анализа рисков информационной безопасности.

Степень изолированности песочницы мы проверяли методикой, имитирующей злонамеренные сетевые атаки, поскольку все решения тестировались в реальной сети - в изолированной сетевой среде, физически - на выделенном сервере, то прежде чем попасть на анализ в песочницу, симуляции блокировались имеющимися у заказчика (колледжа) средствами защиты, с использованием сигнатурных, репутационных и других механизмов.

Результаты тестирования песочницы и настроенных сетевых правил показали высокий уровень безопасности, что доказывает ранее выдвинутую гипотезу по повышении защищенности информационных ресурсов образовательной организации, значимой частью которых являются электронные образовательные ресурсы.

Таким образом, задачи исследования решены, цель достигнута, гипотеза нашла свое подтверждение.

Библиографический список

1. ГОСТ Р 53620 - 2009 «Информационно-коммуникационные технологии в образовании. Электронные образовательные ресурсы. Общие положения».

2. ГОСТ Р 53625-2009 (ИСО/МЭК 19796-1:2005) Информационная технология. Обучение, образование и подготовка. Менеджмент качества, обеспечение качества и метрики. Часть 1. Общий подход

3. ГОСТ Р 57628-2017 Информационная технология (ИТ). Методы и средства обеспечения безопасности.

4. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий [].

5. ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Практические правила управления информационной безопасностью.

6. ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

7. ГОСТ Р ИСО/МЭК 9594-8-98 «Информационная технология (ИТ). Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации».

8. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий».

9. ГОСТ Р 51901.1-2002. Менеджмент риска. Анализ риска технологических систем.

10. ГОСТ Р 51901.12-2007. Метод анализа видов и последовательность отказов [Электронный ресурс]. – Режим доступа: http://www.opengost.ru/iso/13_gosty_iso/13110_gost_iso/4936-gost-r-51901.12-2007-mek-60812_ 2006-menedzhment-riska.-metod-analiza-vidov-i-posledstviy-otkazov.html свободный, дата проверки: 17.12.2018

11. [Электронный ресурс]: Доктрина информационной безопасности Российской Федерации //: URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

12. [Электронный ресурс]: Концепция обеспечения информационной безопасности предприятия URL: http://securitypolicy.ru

13. [Электронный ресурс]: Электронный журнал «ПРАВОВАЯ ИНИЦИАТИВА» ISSN 2304-5655/ Концепция общественной безопасности в РФ как правовая мера безопасности образовательных учреждений (организаций)// http://49e.ru/ru/2014/4/18

14. ФЗ от 27 июля 2006г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»

15. ФЗ от 27.07.2006 №152-ФЗ «О персональных данных».

16. ФЗ от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

17. Абдулин А.А., Гафарова Е.А. Направления обеспечения информационной безопасности электронного документооборота в ГБОУ СПО (ССУЗ) «Челябинский профессиональный колледж».// Информационные технологии Сибири сборник материалов международной научно-практической конференции. Западно-Сибирский научный центр. 2016. С. 87-90.

18. Аргимбаева Ж. Н. Электронный учебный практикум по программированию в среде visual basic // Аргимбаева Ж.Н. - http://collegy.ucoz.ru/publ/26-1-0-9875.

19. Архангельский С.И. Лекции по теории обучения в высшей школе. М.: Высшая школа, 1974. – 385 с. – URL: http://www.guma.oglib.ru/bgl/51.html. Дата обращения 17.03.18.

20. Бабанский Ю.К. Педагогика / Бабанский Ю.К. – М.: «Просвещение», 1983. - 608 с. – URL: http://www.detskiysad.ru/ped/ped142.html

21. Бадарч Дендев. Информационные и коммуникационные технологии в образовании: монография / Под. редакцией: Бадарча Дендева – М. : ИИТО ЮНЕСКО, 2013 – 320 с.

22. Белов, Е.Б. Основы информационной безопасности.//Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2016. – 544 с.

23. Беспалько В. Слагаемые педагогической технологии. - М.: Педагогика, 1989. – URL: http://www.alleng.ru/d/ped/ped020.htm. Дата обращения 16.03.18.

24. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы [Текст] // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). — Уфа: Лето, 2011. — С. 8-13. — URL https://moluch.ru/conf/tech/archive/5/1115/ (дата обращения: 16.01.2019).

25. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы [Текст] // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). — Уфа: Лето, 2011. — С. 8-13. — URL https://moluch.ru/conf/tech/archive/5/1115/ (дата обращения: 16.01.2019).

26. Брень Д.Е. Инновационные технологии и их роль в формировании феномена Google // Известия вузов. Северо-Кавказский регион. Серия: Общественные науки. 2014. №4 (182). URL: https://cyberleninka.ru/article/n/innovatsionnye-tehnologii-i-ih-rol-v-formirovanii-fenomena-google (дата обращения: 13.01.2019)

27. Вуль В.А. Электронные издания. Учебник // В.А. Вуль – URL: http://www.hi-edu.ru/e-books/xbook119/01/part-010.htm. Дата обращения 20.03.18.

28. Гафарова Е.А. О возможности использования открытых лицензий для защиты интеллектуальных прав создателей научных и образовательных ресурсов.// Современное развитие науки: вопросы теории и практики Сборник материалов II-ой международной научно-практической конференции. 2016. С. 46-47.

29. Гафарова Е.А. Синицын Ф.В. К вопросу проектирования онтологий предметной области при подготовке магистров по направлению информационная безопасности.//Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы. Сборник научных трудов. 2016. С. 56-59.

30. Гершунский Б.С. Педагогическая прогностика: методология, теория, практика/Б. С. Гершунский. Киев: Вища шк., 1986. - 200 с. – URL: http://lib.mgppu.ru/OpacUnicode/index.php?url=/notices/index/IdNotice:11585/Source:default. Дата обращения 17.03.18.

31. Зеер Э.Ф. Психология профессионального образования / Э.Ф. Зеер. Учеб. пособие. – М.: Академия, 2013. - 416 с. – URL:http://www.academia-moscow.ru/ftp_share/_books/fragments/fragment_23598.pdf. Дата обращения 14.03.18.

32. Зимняя И.А. Педагогическая психология. Учебное пособие Ростов н/Д.: Феникс, 2001. – URL: http://psychlib.ru/mgppu/zim/zim-001-.htm. Дата обращения 16.03.18.

33. Матыкин В.Ю. Создание и использование электронных учебных пособий. – URL: http://e-lib.gasu.ru/konf/nit/archiv/2005/3/4.html. Дата обращения 16.03.18.

34. Мезенов А.С., Гафарова Е.А. О реализации конституционного права граждан на доступ к информации в условиях интенсификации сетевого взаимодействия/ / А.С. Мезенов, Е.А. Гафарова // Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы : сборник научных трудов. — Челябинск: Челябинский филиал РАНХиГС, 2016. — С. 94–98. — 200 с. — ISBN: 978-591970-052-4.

35. Назарова Т.С., Полат, Е.С. Средства обучения (Технология создания и использования) / Т.С.Назарова, Е.С.Полат. – М.: Изд-во УРАО, 2001. – 203 с. – URL: http://www.monographies.ru/ru/book/section?id=1354. Дата обращения 16.03.18.

36. Полат Е.С. Новые педагогические и информационные технологии в системе образования: учебное пособие / Е.С. Полат, М. Ю. Бухаркина, М.В. Моисеева, А.Е. Петров // Под ред. Е. С. Полат. -4-е изд. — М.: Академия, 2009. 272 с. – URL: http://library.kpi.kharkov.ua/NEW/NewPiITvSO.pdf. Дата обращения 17.03.18.

37. Политика в отношении персональных данных в ГБПОУ «Южно-Уральский государственный технический колледж»[http://sustec.ru/svedeniya-

o-kolledzhe/dokumenty/SMK-PP-72-01-Politika-v-otnoshenii-obrabotki-personalnykh-dannykh.pdf].

38. Положение об обработке и защите персональных данных в ГБПОУ «Южно-Уральский государственный технический колледж»[http://sustec.ru/svedeniya-o-kolledzhe/dokumenty/ SMK-PP-71-01-Ob-obrabotke-i-zashhite-personalnykh-dannykh.pdf]

39. Положение об организации работы по охране труда, обеспечению безопасности образовательного процесса в ГБПОУ].SUOT-PP-02-01-Ob-organizacii-raboty-po-OT-obespecheniyu-bezopasnosti-obrazovatelnogo-processa.pdf],

40. Положение об электронных учебных изданиях (ресурсах). – URL: http://portal.tpu.ru:7777/science/seminar/methodic/info/regulations/e-publish.pdf. Дата обращения 16.03.16

41. Программа развития ЮУрГТК [http://sustec.ru/svedeniya-o-kolledzhe/dokumenty/PROGRAMMA-RAZVITIYA-YUUrGTK-na-2014-2018gg-dlya-chirpo.pdf]

42. Сабанов А.Г. О проблеме достоверности идентификации пользователя при удаленном электронном взаимодействии // Доклады ТУСУР. 2014. №2 (32). URL: https://cyberleninka.ru/article/n/o-probleme-dostovernosti-identifikatsii-polzovatelya-pri-udalennom-elektronnom-vzaimodeystvii (дата обращения: 15.01.2019).

43. Салихов А.Т. Проектирование и разработка электронного практикума // А.Т. Салихов. – URL: http://www.fcoit.ru/internet_conference/the_ development_of_electronic_teaching_materials_in_the_learning_process/proektirovanie_i_razrabotka_elektronnogo_praktikuma.php. Дата обращения 18.03.18.

44. Татаринцев А. И. Электронный учебно-методический комплекс как компонент информационно-образовательной среды педагогического вуза [Текст] // Теория и практика образования в современном мире: материалы междунар. науч. конф. (г. Санкт-Петербург, февраль 2012 г.). — СПб.: Реноме, 2012. — С. 367-370.

45. Техническое руководство по разработке учебно-методического комплекса для системы дистанционного обучения. – СПБ: СПБГУИТ,МиО. – URL: http://de.ifmo.ru/--doc/tz_54.pdf. Дата обращения: 22.03.18.

46. Шемяков А.О. Научно-методический аппарат оценки уязвимости системы обеспечения безопасности информации в современном вузе - диссертация на соискании степени канд. техн. наук, 2013 Серпухов. [Электронный ресурс]: URL: http://www.dissercat.com/content/nauchno-metodicheskii-apparat-otsenki-uyazvimosti-sistemy-obespecheniya-bezopasnosti-informa

47. Щеголева Т.В. Методическое руководство по разработке электронного учебно-методического обеспечения системы электронно-дистанционного обучения / Т.В. Щеголева, В.Г. Юрасов, Г.В. Кольцова - Воронеж: ФГОУ ВПО «ВГТУ», 2012. - 25 с.

48. [Электронный ресурс]: Обеспечение информационной безопасности современного ВУЗа/ А. Лукацкий // URL: http://www.comprice.ru/articles/detail.php?ID=504092

49. [Электронный ресурс]: Положение об электронных образовательных ресурсах Краевого ГБПОУ «Профессиональное образовательное учреждение немецкого национального района»// URL:http://www.proflizei.ru/Akty/p_ob_ehlektronnykh_obraz_resursakh.pdf. - (дата обращения: 02.12.2018).

50. [Электронный ресурс]: Положение об электронных образовательных ресурсах ГОУ ВПО «Дагестанский государственный университет» //URL: http://www.ndoc.dgu.ru/PDFF/8.01.pdf - (дата обращения: 02.12.2018).

51. [Электронный ресурс]:Положение об электронных образовательных ресурсах ФГАОУ ВПО «Сибирский федеральный университет»//: URL: http://about.sfu-kras.ru/docs/8733/pdf/413360 - (дата обращения: 02.12.2018).

52. [Электронный ресурс]: http://sustec.ru

53. Guide to using @Risk. Risk analysis and simulation for Microsoft Exel. -Palisade Corp. 2002. http://www.palisade.com

54. Information technology Security techniques -Evaluation criteria for IT security - Part 1: Introduction and general model.

55. Information technology Security techniques -Evaluation criteria for IT security - Part 2: Security functional requirements.

56. Information technology Security techniques -Evaluation criteria for IT security - Part 3: Security assurance requirements.

57. Olovsson T. A structured approach to computer security. Technical Report № 122, 2012. Dept. of Computer Engineering, Chalmers University of Technology, Sweden. [Электронный ресурс]: http://www.ce.chalmers.se/research/Security/Publications/

58. RiskWatch users manual, - [Электронный ресурс]: http://www.riskwatch.com.

59. Managing the Threat of Denial-of-Service Attacks, CERT-Coordination Center, October 2013.

60. R. Witty, J. Dubiel, J. Girard, J. Graff, A, Hallawell ets. The Price of Information Security. Gartner Research, Strategic Analysis Report, K-l 1-6534, June, 2015.

61. Department of Defense Trusted Computer System Evaliation Criteria ~ DoD 5200.28-STD, 2009

62. Background reading material on intelectual property. World Intellectual Property Organization, 2018 - 464 p.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1

СОДЕРЖАНИЕ ЭЛЕКТРОННОГО ПРАКТИКУМА ПО ИЗУЧЕНИЮ PHP (ИСТОЧНИК – «PHP СОБЕСЕДОВАНИЕ В ВОПРОСАХ И ОТВЕТАХ». АНДРЕЙ ШЕВЧЕНКО)

1. Какая разница между функциями sort(), asort() и ksort()?

1) sort() сортирует массив элементов. В отсортированном массиве элементы размещаются по возрастанию. Это функция сортировки по умолчанию.

2) asort() сортирует ассоциированный массив так, что отсортированными оказываются элемен- ты-значения ассоциаций. Используется, если важен порядок самих элементов, а не ключей.

Например:

$capitals = array(“US” => “Washington”, “UK” => “London”, “Austria” => “Vienna”);
asort($capitals);

// $capitals = {“UK” => “London”, “Austria” => “Vienna”, “US” => “Washington”}

3) ksort() сортирует ассоциированный массив по значению ключей. Для предыдущего примера отсортированные значения были бы такими:

ksort($capitals);

// $capitals = {“Austria” => “Vienna”, “UK” => “London”, “US” => “Washington”}

2. Что такое динамические переменные?

Динамической переменной считается та, имя которой хранится в самой переменной. Это так называемая “переменная переменная”.

Например:

$var = “first”;
$$var = “Second”;

// $$var == $first == “Second”
$$var – динамическая, ее имя может меняться вместе с изменением $var. Также, можно связать имя переменной с содержимым другой переменной неявно:

$first = “second”;
$second = “third”;
print $first; // напечатает “second”
print $$first; // напечатает “third”

3. Какими способами можно перенаправить страницу в PHP?

1. Используя функцию PHP header()

```
header('Location:
        '.$url);
```

2. Используя JavaScript

```
echo '<script type="text/javascript">';
echo
'window.location.href="'.$url.'";';
echo '</script>';
```

4. Назови и опиши пять любых типов ошибок PHP.

E_ERROR. Этот тип ошибок возникает при критичных ошибках, выполнение скрипта немедленно прерывается.

E_WARNING. Предупреждает программиста об ошибке, но выполнение скрипта не останавлива- ется.

E_PARSE. Возникает во время компиляции, такие ошибки обычно генерируются парсером.

E_USER_WARNING. Некритичное предупреждение, которое генерируется пользователем. Устанавливается программистом с помощью trigger_error().

E_COMPILE_WARNING. Генерируется скриптовым движком Zend. Некритичная ошибка компиляции.

Также, в PHP5 доступен новый уровень обработки ошибок – E_STRICT, сообщения которого возникают при использовании устаревших возможностей PHP.

5. В чем различия между четвертой и пятой версиями PHP?

Явно устаревший вопрос, но его почему-то до сих пор задают. Перечислять все, не нужно, достаточно сказать, что:

В пятой версии были добавлены следующие возможности:

– ключевое слово static
– Ключевое слово final
– Абстрактные классы
– Интерфейсы
– Магические методы

6. Что такое тип данных?

Тип данных – это описание, определяющее свойства и порядок обработки данных. Например, фраза "переменная $str имеет тип данных "строка" означает, что в этой переменной может со- держаться любое число символов, а операция сложения строк представляет собой последовательное соединение слагаемых строк в одну.

7. Что можешь сказать про типизацию данных в PHP?

PHP является языком программирования с динамической типизацией, не требующим указания типа при объявлении переменных, равно как и самого объявления переменных. Преобразования между скалярными типами зачастую осуществляются неявно без дополнительных усилий. Впрочем, PHP предоставляет широкие возможности и для явного преобразования типов.

8. Сколько типов данных в PHP?

PHP поддерживает 8 базовых типов данных.

4 скалярных типа:

boolean. Логический тип данных, переменные данного типа могут принимать значения true или false.

integer. Целочисленный тип данных, переменные могут принимать целые значения (...-2, -1, 0, 1, 2...) в диапазоне от -2^31 до +2^31. Если значение превышает данный порог – оно автоматически переводится в тип float.

float. Числовой тип данных с плавающей точкой, может содержать как целые, так и дробные величины.

string. Строковый тип данных. Содержит нефиксированное количество различных символов. PHP не накладывает никаких ограничений на длину строки, поэтому можно смело работать даже с ОЧЕНЬ большими строками.

2 комплексных (составных) типа:

array. Массив, содержит упорядоченный список

элементов. **object.** Объект, содержит некий

объект (экземпляр класса). **2 специальных**

типа:

resource. Ссылка на абстрактный элемент, т.н. внешний ресурс. Примеры внешних ресурсов - ссылка на файл и ссылка на результат выполнения запроса

NULL. Пустой тип данных, обозначающий отсутствие какого-либо значения. О таких значениях обычно говорят “не определено”. Пустым значением можно инициализировать переменные любого другого типа.

9. Что такое static функция и чем она отличается от “обычной” (не static)?

Static принадлежит классу, а не экземпляру класса. И вызывается у класса, а не у объекта, т.е. напрямую.

Объявление свойств и методов класса статическими позволяет обращаться к ним

без создания экземпляра класса. Атрибут класса, объявленный статическим, не может быть доступен посредством экземпляра класса (но статический метод может быть вызван). Так как статические методы вызываются без создания экземпляра класса, то псевдопеременная $this не доступна внутри метода, объявленного статическим.

Доступ к статическим свойствам класса не может быть получен через оператор ->.

10. Есть ли разница между self и this в php?

self используется для статических функций и членов класса, а this наоборот для нестатических.

11. Что такое конструктор?

В PHP (начиная с версии 5) конструктор – это метод__construct(), который автоматически вызы- вается ключевым словом new после создания объекта. Обычно он используется для выполнения различных автоматических инициализаций, как например, инициализация свойств. Конструк- торы также могут принимать аргументы, в этом случае, когда указано выражение new, необхо- димо передать конструктору формальные параметры в круглых скобках.

12. Приведи пример конструктора.

```
<?php
class MyClass {
public function _construct() {
echo “Привет из конструктора!”;
}
}
$myObject = new MyClass();
?>
```

13. Обязательно ли писать ?> в конце скрипта?

Нет

14. В каких случаях это не стоит писать?

Для файлов, содержащих только PHP-код, закрывающий тег ?> лучше не использовать. Он не требуется синтаксисом PHP и его пропуск предотвращает случайное включение в вывод конеч- ных пробелов.

15. Поддерживает ли PHP множественное наследование?

Нет, PHP не поддерживает множественное наследование. То есть у производного класса может быть только один родительский. Но с помощью “магической” функции call() его можно эмули- ровать.

16. Какая разница между require(), require_once(), include() и include_once()?

require() включает в страницу заданный файл, в то время как require_once() делает это только в том случае, если этот файл не был включен ранее (на одной и той же странице).

Таким образом, require_once() лучше использовать, если нужно включить файл с большим коли- чеством функций. Тогда можно быть уверенным, что файл не будет включен многократно и не возникнет ошибка “объявление функции дублируется”.

Отличие между require() и include() следущее: require() возвращает FATAL ERROR, если файл не найден, include() же возвращает только WARNING.

Функция include_once() работает почти так же, как и include(), а отличия те же, что и между require() и require_once().

17. Какая разница между функциями echo и print в PHP?

Во-первых, echo может принимать и выводить любое количество аргументов, а print - только один. Во-вторых, print всегда возвращает 1, поэтому может быть использован в контексте выра- жения.

18. Что делает функция eval()?

eval() вычисляет строку как PHP-код.

19. Чем отличается цикл while от do while?

do-while всегда выполняет тело цикла хотя бы один раз, поскольку его условное выражение про- веряется в конце цикла.

20. Как перевернуть массив? Есть массив array(‘h’, ‘e’, ‘l’, ‘l’, ‘o’), как из него по- лучить array(‘o’, ‘l’, ‘l’, ‘e’, ‘h’)?

Для этого в PHP есть функция array_reverse().

21. А как перевернуть массив без нее?

Например, так:

```
<?php
$arr = array(‘h’, ‘e’, ‘l’, ‘l’, ‘o’);
$reversed = array();
for ($i=0; $i<count($arr); $i++) array_unshift($reversed, $arr[$i]); for
($i=0; $i<count($reversed); $i++) echo “$reversed[$i]”;
?>
```

22. Как перевернуть строку?

Функцией strrev(), а если без нее, то проще всего так:

```
<?php
$str = “Turn me baby”;

for ($i = strlen($str); $i>=0; $i--) $rev[] = $str[$i];
$revstr = implode (“”,
$rev); echo $revstr;
?>
```

А если это слишком просто, то можно и так:

```
<?php
$str = “Turn
me baby”;
function
myrev($src) {
$length = strlen($src);
for ($i = 0; $i < $length / 2; $i++) {
$a = $src[$i];
$src[$i] = $src[$length - $i - 1];
$src[$length - $i - 1] = $a;
}
return $src;
}
echo myrev($str);
?>
```

Или вот еще вариант:

```
<?php
$a = ‘Turn me baby’;
$b = ‘’;
for ($i = strlen($a)-1; $i>=0; $i--)
     $b .=
    $a[$i];
$
a

=

$
b
;

e
c
h
o

$
a
;
```

```
?>
```

23. Что такое рекурсия?

Рекурсия – это вызов функции из неё же самой, непосредственно (простая рекурсия) или через другие функции (сложная или косвенная рекурсия), например, функция A вызывает функцию B, а функция B – функцию A. Количество вложенных вызовов функции или процедуры называется глубиной рекурсии.

24. Напиши пример рекурсивной функции, которая вычисляет факториал числа.

```
<?php
function
fac($x) {
if ($x
=== 0)
return 1;
else
return $x*fac($x-1);
}
echo fac(4);
?>
```

25. Как вывести на экран ряд чисел Фибоначчи?

```
<?php
function fibonacci($n)
{
if ($n < 3) {
return 1;
}
else {
return fibonacci($n-1) + fibonacci($n-2);
}
}
for ($n = 1; $n <= 16; $n++) {
echo(fibonacci($n).“,“);
}
echo(“...\n”)
?>
```

26. Сложение в PHP и JavaScript. ”123” + “abc”. Что будет? А если 123 + ”abc”?

В JavaScript “+” это конкатенация, т.е. строки просто соединятся. В PHP в обоих случая результат будет 123. А если в PHP сложить, например, 10 + ”20”, то, несмотря на кавычки результат будет 30.

27. Есть ли разница между одинарными и двойными кавычками в PHP?

В двойных кавычках данные “парсятся”, а в одинарных – нет. Двойные кавычки в данном случае приведут к результату Chimay, а одинарные к $beer.

```
<?php
$beer =
‘Chima
y’; echo
“$beer”;
?>
```

28. Проход массива. Как вывести все элементы массива на экран?

Вывести с

ключами: print_r.

А пройти и

вывести массив:

```
<?php
$cars = array( “BMW”, “Audi”, “Mercedes”,
“Porsche” ); foreach ($cars as $car) {
  echo $car . “<br />”;
}
?>
```

29. В чём разница между функциями count() и sizeof()?

Функция count() выполняет ту же операцию, что и sizeof() – возвращает количество значений, содержащихся в массиве. Единственное различие между ними заключается в том, что в некото- рых ситуациях count() возвращает дополнительную информацию:

– Если переменная существует и является массивом, count() возвращает количество элементов в массиве;

– Если переменная существует, но не является массивом, функция возвращает значение 1;

– Если переменная не существует, возвращается значение 0.

30. Что такое ассоциативный массив

Массивы, индексами которых являются строки, называются ассоциативными. Индексы ассоциативных массивов называются ключами. Например:

```
$people[“Иванов”] = “Иван”;
$people[“Сидоров”] = “Николай”;
$people[“Петров”] = “Петр”;
```

31. Нарисуй форму для отправки файла:

Для реализации возможности загрузки файлов на сервер можно использовать простую форму:

```
<form action=action.php method=post enctype=multipart/form-data>
<input type=file name=uploadfile>
<input type=submit value=Загрузить>
</form>
```

Этот код выводит в браузер элемент input с кнопкой «Обзор» и кнопку «Загрузить». По нажатию на эту кнопку происходит обращение к файлу upload.php, который содержит следующий код:

```
<?php
$uploadfile = './upload/'.basename($_FILES['uploadfile']['name']);
// Копируем файл из каталога для временного хранения
файлов: if (copy($_FILES['uploadfile']['tmp_name'],
$uploadfile))
{
echo "<h3>Файл успешно загружен на сервер</h3>";
}
else { echo "<h3>Ошибка! Не удалось загрузить файл на сервер!</h3>"; exit; }
?>
```

32. Пусть имеем HTML-форму, которая содержит одно поле ввода text и одно поле ввода textarea. Требуется создать для данной HTML-формы скрипт-об- работчик script1.php, который заносит построчно в файл data.txt данные. В итоге структура получаемого файла data.txt должна быть следующая:

```
t
e
x
t
1

t
e
x
t
2

t
e
x
t
3

t
```

e
x
t
4

где столбцы text1 и text3 относятся к полю text, а text2 и text4 к полю textarea. После того, как обработчик script1.php поместит данные в файл, он должен

возвратить пользователя обратно в index.html.

Форма:

```
<html>
<title>Go</title>
<body>
<form action=”action.php” method=”post”>
Введите имя: <input type=”text”
name=”name” /> Сообщение: <input
type=”text” name=”message”/>
<input type=”submit” value=”Ввести” />
</form>
</body>
</html>
```

Файл обработки:

```
<?php
$all=”Name: “.$_POST[‘name’].”\r\n”.”Message: “.$_POST[‘message’].”\r\n”;
$files=”bamb.txt”;
if (!$handle = fopen($files, ‘a’)) {
echo “Не могу открыть файл
($filename)”; exit;
}
if (fwrite($handle, $all) === FALSE) {
echo “Не могу произвести запись в файл ($files)”;
exit;
}
?>
```

33. Используя конструкцию switch, написать функцию boo, принимающую одно число в качестве аргумента. Если это число равно 2, функция должна вывести слово “Двойка”, если 3 – “Тройка”, в остальных случаях – “Фигня ка- кая-то”.

```
<?php
function boo($num) {
switch($num) {

case “2”:
```

```
echo “two!”;
break;

case “3”:
echo “three!”;
break;

default:
echo “shnyaga!”;
break;
}
}
boo(2);
?>
```

34. Дан массив $arr = array(3,8,15,25,16,11,10,5,7,30). Вывести циклом индек- сы тех его элементов, которые делятся на 5.

```
<?php
$arr = array(3,8,15,25,16,11,10,5,7,30);
for ($i=0; $i<=count($arr);
$i++) { if ($arr[$i]%5 == 0) {
echo $arr[$i].”</br>”;
}
}
?>
```

35. Написать программу, которая выводит простые числа, т.е. делящиеся только на себя и на 1.

```
<?php
$lst = array();
$k = “prostoe”;
for($i = 2; $i<100;
$i++) { for($j = 2; $j
< $i; $j++) { if( ($i %
$j) == 0) {
$k=”ne prostoe”;
}
}
if ($k == “prostoe”)
$l
st
[]
=
$i
;
el
se
```

```
$k = “prostoe”;
}
foreach ($lst as $list) echo $list.”</br>”;
?>
```

P.S. В качестве флага ($k) правильнее было бы использовать true/false, но я оставил так как есть, чтобы было легче понять как оно работает.

36. Сгенерировать 3 случайных числа в диапазоне от 0 до 10. Если сумма этих чисел меньше 14, сгенерировать новую тройку.

```
<
?
p
h
p

d
o

{
$a = rand(0, 10);
$b = rand(0, 10);
$c = rand(0, 10);
$result =
$a+$b+$c;
echo
$result.”</br
>”;
}
while ($a + $b + $c < 14);
?>
```

37. Чем отличается передача параметра по значению от передачи по ссылке.

Параметры в процедуры и функции можно передавать 2 способами – по значению и по ссыл- ке. Отличия между этими двумя способами следующие: при передаче параметра по значению в процедуру (функцию) передается копия переменной, а при передаче по ссылке – оригинал (сама переменная).

38. Чему будет равно $a?

```
$a = “1”;
$a[$a]
= “2”;
echo
$a;
```

12

39. Есть массив a = array(тут много элементов). Проходим по массиву циклом for (i=0; i<=count(a); i++). Можно ли как-нибудь ускорить цикл?

Да.

1) Вынести count(a) в отдельную переменную;
2) Считать массив с конца циклом for (i=count(a); i>=0; i--).

40. Вывести максимальное значение элемента массива array(1,2,3,4,10,100,3, 4987,6,7,8,9).

С использованием стандартной функции max():

```
$arr =array(1,2,3,4,10,100,3,4987,6,7,8,9);
echo max($arr);
```

Без использования стандартной функции:

```
<?php
$arr = array(5,45,3,4,5,490,62);
$max =
$arr[0];
foreach ($arr
as $val)
if ($max < $val) $max =
$val; echo $max;
?>
```

41. Напиши программу-цензор, которая бы заменяла вводимые пользовате- лем в форму слова “fuck”, “idiot” и “bitch” на “fk”, “id**t” и “bi**h”.**

```
<?php

$find = array(‘fuck’, ‘idiot’, ‘bitch’);
$replace = array(‘f**k’, ‘id**t’, ‘bi**h’);

If (isset($_POST[‘user_input’]) && !empty($_POST[‘user_input’])) {

$user_input = $_POST[‘user_input’];
$user_input_new = str_ireplace($find, $replace, $user_input);
echo $user_input_new;
}
?>

<html>
<head></head>
<
b
```

```
o
d
y
>

<form action=”a.php” method=”POST”>
<textarea name = “user_input” rows = “6” cols = “30”></textarea>
<input type = “submit” value = “Submit!”>
</form>

</body>
</html>
```

42. Какие магические методы знаешь? Что это вообще такое?

Это методы зарезервированные в php, которые начинаются с двойного подчеркивания “_”.

Список всех магических методов:

__construct
__destruct
__call
__callStatic
__get
__set
__isset
__unset
__sleep
__wakeup
__toString
__set_state
__clone

__construct и_destruct – самые популярные методы, которые реализуют базовые понятия объ- ектно-ориентированного программирования: конструктор и деструктор;

__call,_callStatic,__get и__set – методы, связанные с перегрузкой обращений как к свойствам, так и к методам. Методы__get() и__set() вызываются при установке и получении значения свойства, а методы__call() и__callStatic – при вызове метода. Стоит заметить, что эти магические функции будут вызываться только и исключительно в том случае, если запрошенные метод или свойство не существуют;

__isset – метод, срабатывающий при вызове функций empty() или isset() на несуществующем или недоступном свойстве класса;

__unset – срабатывает при вызове функции unset() на несуществующем или недоступном свойс- тве класса sleep и__wakeup – методы, которые вызываются только из функций serialize и unserialize со- ответственно. Метод__sleep будет

вызван сразу при применении к объекту функции serialize, а метод_wakeup – при применении unserialize. В настоящий момент методы применяются для сохранения текущего состояния системы с последующим восстановлением данного состояния (например, коннект к базе);

toString – метод, с помощью которого можно обращаться к классу как к строке (например, с помощью print или echo);

__set_state – метод, который вызывается для классов, экспортирующих значения свойств функ- цией var_export();

__clone – вызывается при клонировании объекта (введен для использования из-за того, что объ- екты в php5 и выше передаются по ссылке);invoke – вызывается при попытке использовать объект в качестве функции

ПРИЛОЖЕНИЕ 2

Оценочный лист качества педагогического программного средства (образец)

Эксперт (Ф.И.0., должность, звание) _____

_____

Дата _____

Баллы _____(оценка по пятибалльной системе - от 1 до 5)

1. Технический уровень (соответствие техническим требованиям к ППС)		
1.1. Прогон программы (запуск, ввод данных, управление, вывод информации)		
Действия	*Требуемый результат*	*Баллы*
1.1.1. Запуск программы	Заставка отображается	
1.1.2. Вызов блока теоретического материала	Открытие окна с встроенным HTML – пособием	
1.1.3. Вызов блока материала практических работ	Открытие окна с встроенным HTML – пособием	
1.1.4. Запуск тестов самоконтроля	Открытие окна начала теста	
1.1.5. Вызов справки	Отображение справки	
1.1.6. Запуск итогового теста	Открытие формы итогового теста	
1.1.7. Корректное отображение текста в программе	Текст должен отображаться без ошибок	
1.1.8. Ввод данных при регистрации в итоговом тесте	Сохранение данных пользователя и активация управляющих кнопок перехода к тестированию и к работе по рабочей тетради	
1.1.9. Проверка записи данных в текстовые файлы после прохождения итогового теста	Данные должны записываться в текстовой файл	
1.1.10. Вывод информации об оценке и количестве правильных ответов при окончании прохождения теста	Вывод информации на форму теста.	
1.1.11. Работа управляющих кнопок программы	Немедленное выполнение команды указанной на управляющей кнопке	
	Средняя оценка по пункту 1.1.	

2. Эргономический уровень (соответствие эргономическим требованиям к ППС)		
2.1. Сервис пользователя		
Действия	*Требуемый результат*	*Баллы*
2.1.1. Наличие иерархических меню (легкость доступа к информации)	Присутствие иерархических меню в теоретическом и практическом разделах	
2.1.2. Наличие описания возможностей программы	Обеспечивается разделом «Пояснительная записка»	
2.1.3. Легкость навигации	Обеспечивается с помощью управляющих кнопок	
	Средняя оценка по пункту 2.1.	
2.2. Качественность представления информации на экране		
2.2.1. Представление информации в соответствии с эргономическими требованиями	Представление информации соответствует эргономическим требованиям (монитор с размером диагонали экрана не менее 15 дюймов)	
2.2.2. Четкость изображения	Изображение чёткое	
2.2.3. Оптимальное распределение информации на экране, дизайн	Дизайн обеспечивает оптимальное распределение информации на экране	
2.2.4. Представление графических форм в соответствии с возможностями современной компьютерной графики	Наличие графических форм в теоретическом разделе	
	Средняя оценка по пункту 2.2.	
3. Педагогический уровень (соответствие педагогическим требованиям к ППС)		
3.1. Цели использования ППС, методы обучения с использованием ПС		
Действия	*Требуемый результат*	*Баллы*
3.1.1. Отражение в ППС современного состояния научных и педагогических знаний	Учебный материал соответствует современному состоянию научных и педагогических знаний и способствует формированию у обучающегося соответствующих компетенций	

3.1.2. Обоснованность выбора педагогических целей использования ППС и содержания учебного материала	Соответствие особенностям дистанционного обучения. Соответствие требованиям ФГОС третьего поколения.	
3.1.3. Наличие новых организационных форм и методов обучения, поддерживаемых средствами новых информационных технологий	Применение электронного практикума с возможностью записи проделанной работы в текстовые файлы	
3.1.4. Образовательная ценность (соответствие дидактическим требованиям к ППС)	Данное ППС является обучающей и контролирующей программой, предполагающей большую самостоятельность обучающегося.	
	Средняя оценка по пункту 3.1.	
3.2. Форма представления учебного материала (графика, таблицы, текст, рисунки, схемы, картинки и др.).		
Действия	*Требуемый результат*	*Баллы*
3.2.1.Оптимальность взаимосвязи между формой представления учебного материала и его содержанием	Обеспечена оптимальная взаимосвязь между формой представления учебного материала и его содержанием: материал, требующий графического или табличного представления, представлен в соответствующей форме, текст, требующий дополнительных средств, облегчающих восприятие, снабжён рисунками, графиками и т.д.	
3.2.2. Надежность сохранности формы представления и порядка прогона программы от несанкционированного нажатия клавиш	Сохранность от несанкционированного нажатия клавиш обеспечивается последовательной активацией управляющих кнопок в формах рабочей тетради и теста, а также защитой текстовых записей от внесения изменений на формах рабочей тетради, в пояснительной записке и на форме "Почта"	
	Средняя оценка по пункту3.2.	
3.3. Психолого-педагогическое воздействие		
3.3.1. Формирование мышления	Обеспечивается формирование мышления	
3.3.2. Формирование учебного опыта самостоятельного приобретения знаний, умений, навыков	Обеспечивается формирование учебного опыта самостоятельного приобретения знаний, умений, навыков	

3.3.3. Приобретение учебного опыта экспериментально-исследовательской деятельности	Обеспечивается приобретение учебного опыта экспериментально-исследовательской деятельности	
Средняя оценка по пункту 3.3.		
4. Уровень интерактивности		
4.1. Возможность обеспечения обратной связи		
4.1.1. Наличие вариантов ответа	Обеспечивается в тестах	
4.1.2 Наличие возможности диагностики ошибок по результатам учебной деятельности	Обеспечивается в тестах для самоконтроля (активация правильного варианта после прохождения теста)	
4.1.3. Использование совместно с ППС учебного назначения других средств обучения	Возможно	
4.1.4. Содействие развитию сотрудничества между учащимися (групповая, коллективная учебная или досуговая деятельность)	Обеспечивается	
Средняя оценка по пункту 4.1.		
5. Итоговая оценка		
6. Итоговое заключение эксперта		
6.1. Наличие эмпирических или критериальных данных о повышении эффективности процесса обучения, развитии личности обучаемого		
6.2. Возможность применения ППС в реальном учебном процессе		
6.3. Достижимость поставленных педагогических целей		