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

Создание и использование электронного образовательного ресурса в составе информационно-методического обеспечения учебного процесса в условиях реализации политики информационной безопасности

Выпускная квалификационная работа
по направлению 44.04.04 Профессиональное обучение

Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения очная

Проверка на объём заимствований:
73 % авторского текста

Работа рекомендована к защите
«27» мая 2020 г.
Заведующий кафедрой АТИТиМОТД
_____ В.В. Руднев

Выполнил:
магистрант группы ОФ-209/210-2-1,
Шлапакова Дарья Сергеевна
Научный руководитель:
к.т.н., доцент
кафедры АТ, ИТ и МОТД
Руднев Валерий Валентинович

Челябинск, 2020

Оглавление

ВВЕДЕНИЕ 3
ГЛАВА 1. ТЕОРЕТИКО-МЕТОДИЧЕСКИЕ ОБОСНОВАНИЯ СОЗДАНИЯ ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА 9
1.1 Понятие, виды и значение электронного образовательного ресурса в условиях профессионального образования 9
1.2 Этапы разработки электронного образовательного ресурса 11
1.3 Структура разработанного программного продукта 15
ГЛАВА 2. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЮЖНО-УРАЛЬСКОГО ГОСУДАРСТВЕННОГО КОЛЛЕДЖА 28
2.1 Понятие политики информационной безопасности, обзор нормативной документации в Российской Федерации 28
2.2 Реализация политики информационной безопасности в ГБПОУ «Южно-Уральский государственный колледж» 50
ГЛАВА 3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА В КОЛЛЕДЖЕ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 61
3.1. Особенности и ограничения на электронные образовательные ресурсы согласно требованиям информационной безопасности 61
3.2. Рекомендаций по защите электронного образовательного ресурса по профессиональному модулю «Обработка отраслевой информации» в ГБПОУ «Южно-Уральский государственный колледж» 67
3.3. Экспериментальная проверка электронного образовательного ресурса по профессиональному модулю «Обработка отраслевой информации» в ГБПОУ «Южно-Уральский государственный колледж» 72
Выводы по Главе III 75
ЗАКЛЮЧЕНИЕ 76
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 77

ВВЕДЕНИЕ

Актуальность исследования. Научно-технический прогресс, внедрение информационных и коммуникационных технологий (ИКТ) в различные сферы деятельности человека, необходимость постоянного повышения квалификации предъявляют новые требования к подготовке будущих специалистов в условиях цифровизации образования. Одним из приоритетных направлений цифровизации образования становится поиск форм, методов и средств обучения, обеспечивающих более широкие возможности развития и самореализации личности, а также формирование компетентности специалиста, способного организовать учебную и профессиональную деятельность с применением ИКТ и цифровых ресурсов.

В работах Ежовой Г.Л., Лавиной Т.А., Мартиросян Л.П., Образцова П.И., Прозоровой Ю.А., Роберт И.В. и др. отмечено, что использование средств ИКТ, в частности электронных образовательных ресурсов (ЭОР), способствует осуществлению информационной деятельности и информационного взаимодействия на основе незамедлительной обратной связи, интерактивного диалога, автоматизации контроля результатов обучения, реализации информационно-методического обеспечения учебно-воспитательного процесса (И.В. Роберт). Использование электронных образовательных ресурсов позволяет также обеспечить на более высоком уровне индивидуализацию обучения, изменяя методы и формы обучения, создать условия для формирования практических умений и навыков самостоятельной работы.

В настоящее время информатизация образования рассматривается как процесс интеллектуализации деятельности обучающего и обучаемого, как погружение человека в новую интеллектуальную среду. К перспективным направлениям информатизации образования

отнесены: разработка и оптимальное использование средств информационных и коммуникационных технологий (ИКТ), а именно электронных образовательных ресурсов (ЭОР), и расширение масштабов их внедрения в учебный процесс. Методическая система формирования профессиональной компетентности студентов колледжа описывает модель методической системы, ее структурные элементы, иерархические связи между ними, этапы и виды образовательной деятельности главных участников образовательного процесса: студента и преподавателя.

В работах Роберт И.В., Аверьяновой Т.А., Николаевой Н.В. и др. отмечается, что учебная деятельность, выполняемая с использованием средств ИКТ, основана на осуществлении информационной деятельности и информационного взаимодействия между обучающимся, преподавателем и интерактивными средствами ИКТ и направлена на достижение учебно-профессиональных целей.

Достижения, имеющиеся в настоящее время в области применения ЭОР, обусловлены, прежде всего, высоким уровнем аппаратного и программного обеспечения современных ИКТ.

Основываясь на исследованиях Александровой Н.В., Геркушенко Г.Г., Горневой Е.А., Гура В.В. и др., можно говорить о том, что создание и использование ЭОР должно соответствовать требованиям обеспечения целостности учебного процесса, единства педагогических целей развития личности, содержания, форм, методов обучения и обеспечивать учебно-методическую и психолого-педагогическую поддержку учебной деятельности. В исследованиях в области комплексного применения средств ИКТ в обучении (Горнева Е.А., Короткова И.И., Скабеева Л.И, Скарга В.А., Тарабрин О.А. и др.) подчеркивается необходимость разработки информационно-методического обеспечения учебной деятельности на основе взаимосвязанного использования учебно-методических материалов на

базе ИКТ и реализации дидактических возможностей ИКТ (И.В. Роберт).

Внедрение инновационных образовательных стандартов и программ, компьютеризация и подключение всех образовательных организаций к сети интернет, использование электронных образовательных ресурсов в практике обучения и управления образованием – далеко неполный перечень обязательно проводимых мероприятий в каждой образовательной организации, необходимых для создания информационного единства в колледже.

Вот поэтому-то обеспечение информационной безопасности учебного процесса, в том числе непрерывного функционирования компьютерных и электронных образовательных ресурсов, является весьма важной для его качества.

Относительно образовательных организаций под информационной безопасностью понимают – защищенность информации от любого (случайного или преднамеренного) несанкционированного вмешательства (попыток хищения, модификации и т.п.). Безопасность, рассматриваемой системы, определяется конфиденциальностью, целостностью и доступностью компонентов.

Защищаемая информация включает в себя комплекс мероприятий, которые проводятся собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации, а также к ее носителям.

Таким образом*, проблема исследования* заключается в обеспечении информационной безопасности электронных образовательных ресурсов в составе информационно-методического обеспечения учебного процесса колледжа.

Целью исследования является теоретически обосновать и проверить эффективность электронного образовательного ресурса в составе информационно-методического обеспечения учебного процесса образовательной организации в условиях обеспечения информационной безопасности.

Объект исследования: учебно-методическое обеспечение профессиональной подготовки студентов среднего профессионального образования для организации самостоятельной работы в образовательной организации.

*Предмет исследования***:** процесс применения электронного образовательного ресурса в образовательном процессе организации СПО в условиях информационной безопасности.

Гипотеза исследования: Гипотеза исследования состоит в предположении о повышении защищенности электронных образовательных ресурсов образовательной организации при выполнении комплекса требований:

- настройка политики безопасности сайта;
- распределение прав доступа к файлам;
- применение SQL-инъекции;
- использование скрипта для запрета копирования, запрет выделения текста в CSS-стилях.

В соответствии с объектом, предметом и целью исследования были поставлены следующие **задачи:**

– изучить понятие, виды и требования, предъявляемые к электронным образовательным ресурсам;

– описать обеспечение информационной безопасности образовательного процесса в ГБПОУ «Южно-Уральский государственный колледж»;

– разработать структуру электронного образовательного ресурса по профессиональному модулю «Обработка отраслевой информации» в

соответствии с содержанием и порядком организации самостоятельной работы студентов;

– разработать рекомендации по защите электронных образовательных ресурсов в ГБПОУ «Южно-Уральский государственный колледж» на основе апробации ЭОР.

Методологическая основа исследования:

- работы по системно-деятельностному подходу (Л.С. Выготский, Л.В. Занков, А.Р. Лурия, Д.Б. Эльконин, В.В. Давыдов);

- положения исследований в области проектирования педагогических технологий (В.П. Беспалько и другие);

- теория информатизации образования (И.В. Роберт, Е.И. Машбиц, М.П. Лапчик и др.);

- работы по компетентностному подходу в образовании (Д.Г. Арсеньев, В.И. Байденко, И.М. Осмоловская);

- законодательные и нормативно-правовые документы РФ.

Научная новизна и теоретическая значимость исследования заключается в определении функционала и структуры электронных образовательных ресурсов для организации самостоятельной работы студентов в условиях реализации информационной безопасности колледжа.

Практическая значимость работы заключается в апробации и внедрении электронных образовательных ресурсов для организации самостоятельной работы студентов колледжа, выявление и устранение угроз информационной безопасности.

Апробация исследования:

База исследования: ГБПОУ «Южно-Уральский государственный колледж».

Структура работы: магистерская диссертация состоит из введения, трех глав, заключения, списка использованных источников,

состоящего из 61 наименований. Работа содержит 16 рисунков. Общий объем работы составляет 66 страниц.

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДИЧЕСКИЕ ОБОСНОВАНИЯ СОЗДАНИЯ ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА

1.1 Понятие, виды и значение электронного образовательного ресурса в условиях профессионального образования

Развитие информационных технологий обусловило появление новой формы образования – электронное образование (e-learning), то есть обучение с использованием информационно-коммуникационных технологий. Основой электронного образования являются электронные образовательные ресурсы [1].

Под электронным образовательным ресурсом понимают образовательный ресурс, представленный в электронно-цифровой форме (ГОСТ 52653-2006), для использования которого необходимы средства вычислительной техники. В общем случае образовательный ресурс включает в себя структуру, предметное содержание и метаданные о них.

Электронные образовательные ресурсы являются элементом модернизации современного образовательного пространства, ориентированы на использование ресурсов сети Internet и повышение уровня профессиональной культуры специалиста.Современные исследования в области эффективности электронных ресурсов и технологий в образовательном процессе позволяют выстраивать приоритеты развития педагогических технологий. [21]

Виды образовательных ресурсов

В электронном обучении основой электронного образовательного ресурса является образовательный контент. Метаданные электронного образовательного ресурса содержат стандартизированную информацию, необходимую для поиска ресурса посредством технологической системы обучения.

Система электронных образовательных ресурсов, информационных образовательных сервисов, средств, технологий,

созданных на программно-аппаратной платформе, которая обеспечивает использование электронных ресурсов и сервисов в образовательных целях, представляет собой информационную образовательную систему (другое часто используемое название – автоматизированная обучающая система).

Контент электронного образовательного ресурса, прошедший редакционно-издательскую обработку, имеющий выходные сведения и предназначенный для распространения в неизменном виде, является электронным изданием (ГОСТ 7.60-2003). Контент электронного образовательного ресурса может быть представлен в виде:

- учебника – издания, содержащего систематическое изложение учебной дисциплины, ее раздела, части, соответствующих учебной программе, и официально утвержденного для использования в образовательном процессе соответствующего уровня образования;
- учебного пособия – издания, дополняющего или заменяющего частично, или полностью учебник и официально утвержденного для использования в образовательном процессе соответствующего уровня образования;
- учебно-методического пособия – издания, содержащего материалы по методике преподавания и изучения учебной дисциплины, ее раздела или части;
- учебного наглядного пособия – издания, содержащего, как правило, изобразительные материалы в помощь изучению и преподаванию;
- самоучителя – издания для самостоятельного изучения учебного материала без помощи руководителя;
- практикума – издания, содержащего практические задания и упражнения, способствующие усвоению пройденного.

Кроме того, к электронному образовательному ресурсу следует отнести компьютерные обучающие программы и автоматизированные

учебные курсы, официально не определенные ГОСТами. Компьютерная обучающая программа обычно представляет собой систематизированное изложение определенного учебного материала для изучения одного вопроса учебной программы, включающего текстовый, иллюстративный (в том числе мультимедийный) учебный материал, гиперссылки, контрольные вопросы. Компьютерные обучающие программы предназначаются как для самостоятельной работы обучающихся, так и для работы под руководством преподавателя. Компьютерные обучающие программы, кроме приобретения знаний, могут обеспечивать и получение некоторых умений и навыков. Компьютерные обучающие программы, направленные на изучение некоторого раздела учебной программы, объединяются в автоматизированные учебные курсы, которые являются электронными учебно-методическими комплексами

1.2 Этапы разработки электронного образовательного ресурса

Разработка программных продуктов, в том числе и электронных образовательных ресурсов, происходит по этапам жизненного цикла разработки программных продуктов.

При разработке электронного приложения применялся каскадный жизненный цикл разработки прикладных программных продуктов. Каскадная модель предусматривает последовательное выполнение всех этапов проекта в строго фиксированном порядке. Переход на следующий этап означает полное завершение работ на предыдущем этапе.

Данная модель состоит из следующих этапов:

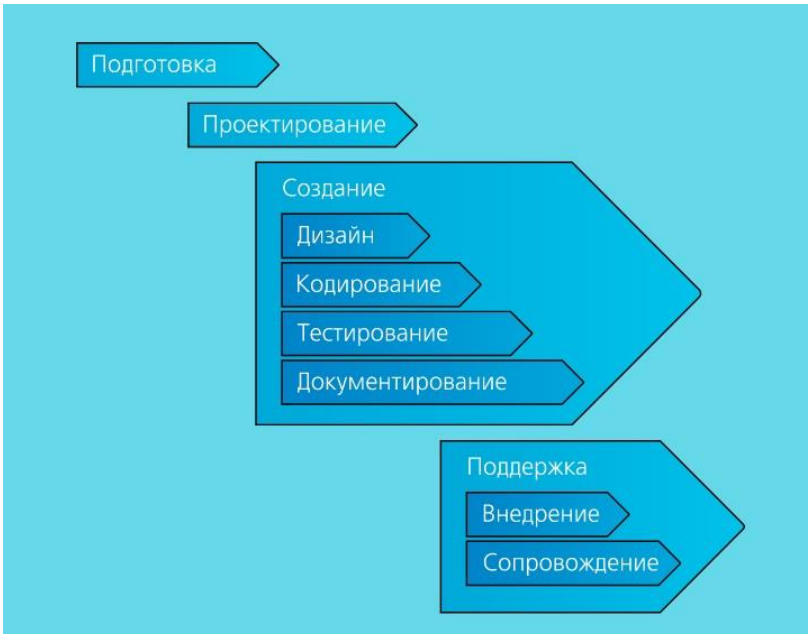


Рисунок 1 — Этапы каскадной модели жизненного цикла

1. Подготовка. На данном этапе мы придумали игру для занятия, которая предполагает разделение группы студентов на 4 команды по 5 человек. Определили, что игра состоит из 5 этапов, что для разработки игровых этапов будем использовать следующие онлайн - сервисы разработки игр: JigsawPlanet, LearningApps, GoogleФормы и – TurboSite для объединения всех разработок в одну программную оболочку.

2. Проектирование. На этапе проектирование мы продумали сценарий и ход игры, описали станции с заданиями, изученными в профессиональном модулем ПМ.01 «Обработка отраслевой информации», определили необходимые ресурсы для проведения игры, также уточнили функции участников, жюри и помощников игры.

3. Создание. Данный этап – непосредственное создание игры в программной оболочке. Дизайн — продумывание стиля и оформления игры, кодирование — написание исходного кода, тестирование — проверка программы на соответствие всем предъявляемым к ней требованиям, документирование — передача накопленных знаний пользователям и другим разработчикам.

Прежде чем объединить все имеющиеся этапы игры в одну оболочку, безусловно, необходимо разработать каждую игру по отдельности.

Для проверки знаний на память, воспроизведения информации была идея создания паззл. Для решения данных задач был использован сервис - Jigsaw Planet - удобный и бесплатный продукт по созданию паззл.

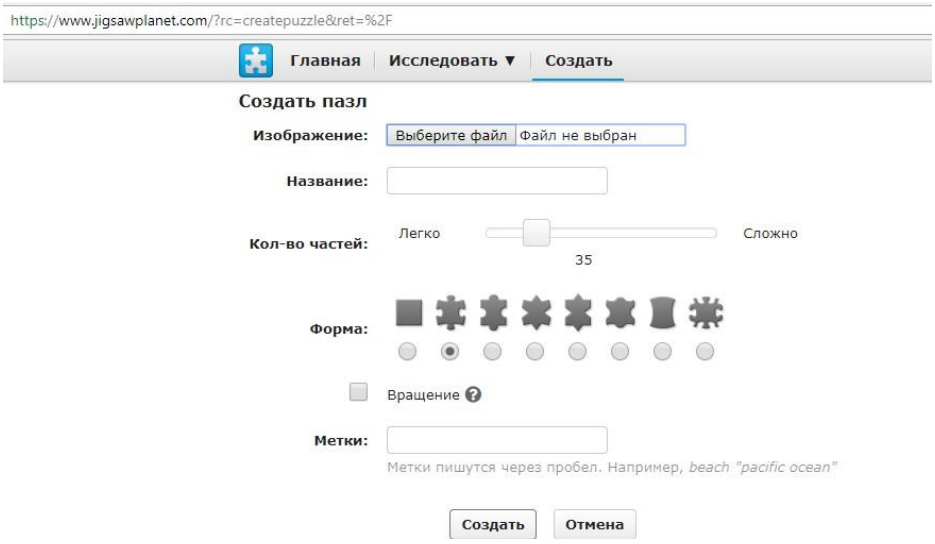


Рисунок 2 — Jigsaw Planet. Рабочее пространство

Также, необходимы были задания обобщения и сравнительного, сопоставляющего и обучающего характера. Сервис LearningApps имеет множество шаблонов по созданию игровых упражнений. Применимо к заданиям нашей разработки, мы использовали следующие упражнения: «Паззлы», «Классификация», «Сортировка картинок», «Слова из букв».

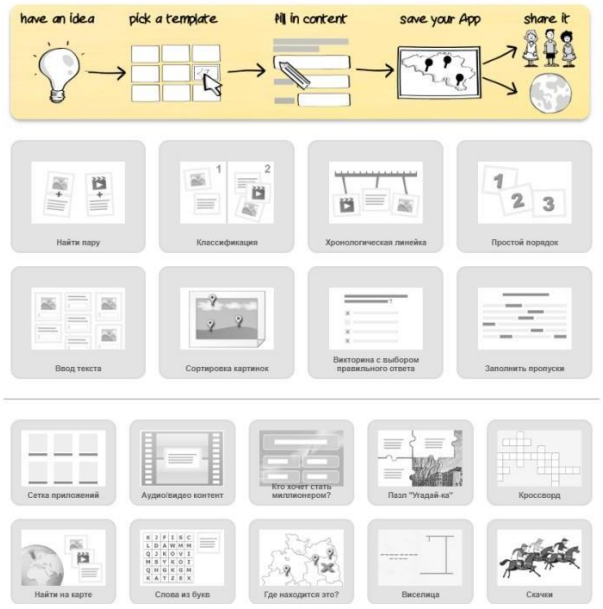


Рисунок 3 — LearningApps. Выбор упражнения

Так как разработанные этапы имеются в различных программных сервисах, необходимо объеденить их в одну оболочку для удобного пользования. Мы решили использовать программное обеспечение «TurboSite» - бесплатная программа лдя создания сайтов и электронных учебников. Данная программа абсолютно не требует ни огромных вычислительных ресурсов компьютера, ни постороннего программного обеспечения. Кроме того, она сконфигурирована таким образом, чтобы работать из любого каталога. Для её запуска достаточно перенести рабочий каталог с лазерного диска в любое место вашего компьютера или запустить ее с лазерного диска.

Каждому этапу присвоили название и отдельную страницу, нажатие на ссылку с названием этапа будет перенаправлено на непосредственный этап игры.

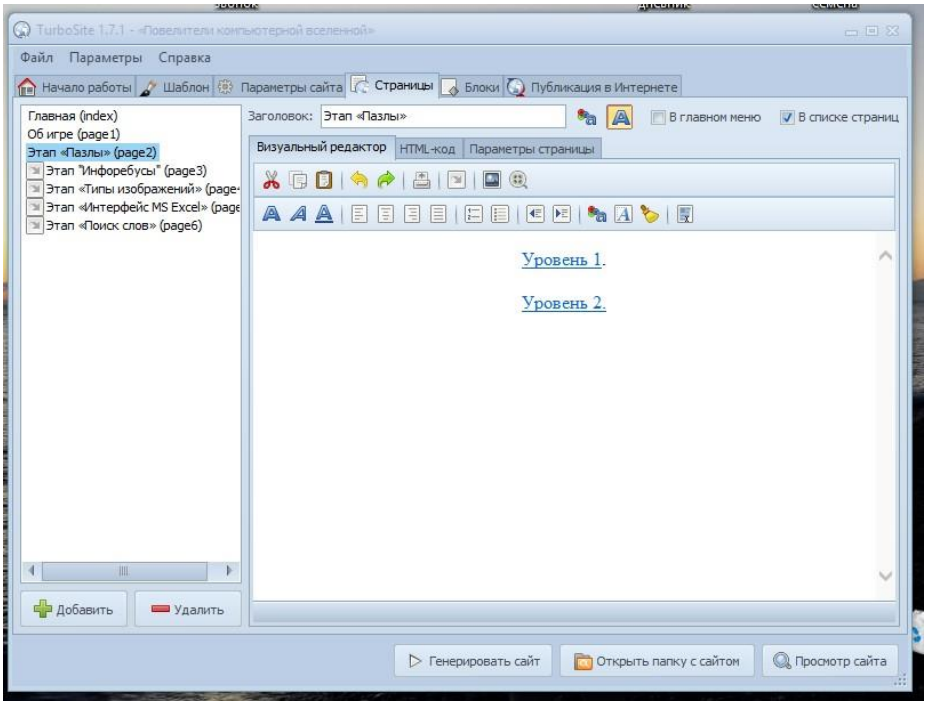


Рисунок 4 — TurboSite. Проектирование игры

Поддержка. На данном этапе происходит непосредственное внедрение электронного приложения игры — установка программного обеспечения, обучение помощников работы с программным продуктом.

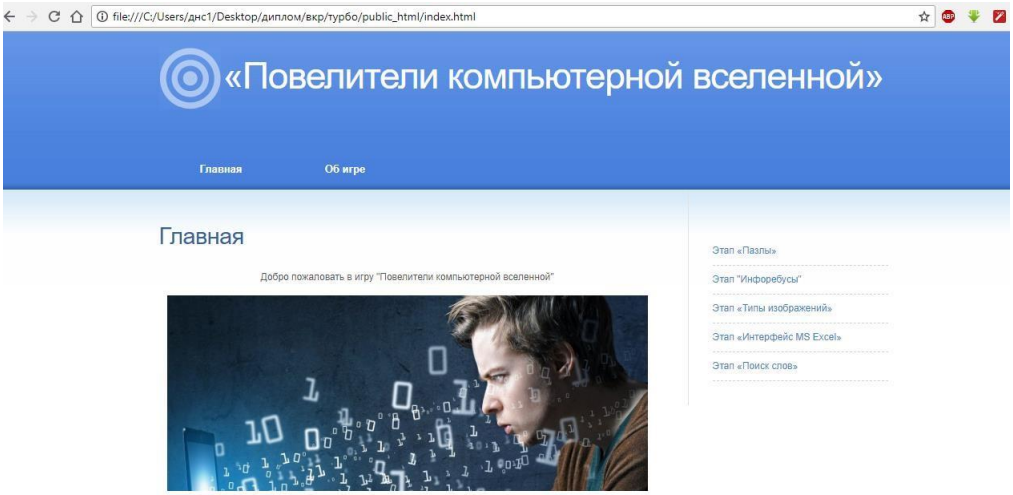


Рисунок 5 — TurboSite. Главная страница игры

1.3 Структура разработанного программного продукта

В качестве электронного образовательного ресурса, для организации самостоятельной работы студентов на занятии по ПМ.01

«Обработка отраслевой информации» требует разработки учебно-методического обеспечения.

Учебно-методическое обеспечение – это совокупность всех учебно-методических документов (планов, программ, методик, учебных пособий и т.д.), представляющих собой проект системного описания образовательного процесса, который впоследствии будет реализован на практике [28].

Для проведения занятия по профессиональному модулю ПМ.01 «Обработка отраслевой информации» была выбрана такая игровая технология, как деловая игра. Для организации и проведения деловой игры необходимо разработать следующее учебно-методическое обеспечение (таблица 1).

Таблица 1 – Элементы учебно-методического обеспечения

Учебно-методическое обеспечение	
Для педагога	Для обучающихся
Инструкция для проведения деловой игры «Повелители информационной вселенной» для организации самостоятельной работы студентов колледжа по профессиональному модулю	Маршрутный лист этапов прохождения деловой игры
	Памятка помощнику «Выставление баллов командам на этапах»
Сценарий деловой игры «Повелители информационной вселенной»	Анкета «Выявление результатов проведения деловой игры Повелители информационной вселенной»
	Электронное приложение деловой игры

Данное учебно-методическое обеспечение позволяет организовать и провести деловую игру по профессиональному модулю ПМ.01 «Обработка отраслевой информации». Полный комплект учебно-методического обеспечения для организации и проведения деловой игры представлено в Приложении 1. Основным и центральным документом учебно-методического обеспечения является описание деловой игры.

Описание деловой игры

Название: «Повелители компьютерной вселенной»

Этапы проведения: Игра состоит из нескольких этапов, на которых командам предлагаются различные задания, позволяющие взглянуть под творческим углом на задачи по обработке отраслей информации, которые стоят перед специалистами среднего звена в области прикладной информатики. Разделение учебной группы из 25 человек на четыре команды происходит случайным образом. Первым делом педагог объявляет обучающимся о необходимости выбрать, по желанию, пять помощников, которые будут ответственными на этапе с заданием. Далее студенты выбирают капитанов будущих команд, которым вручаются случайно выбранные фигуры (квадрат, треугольник, круг, звездочка).

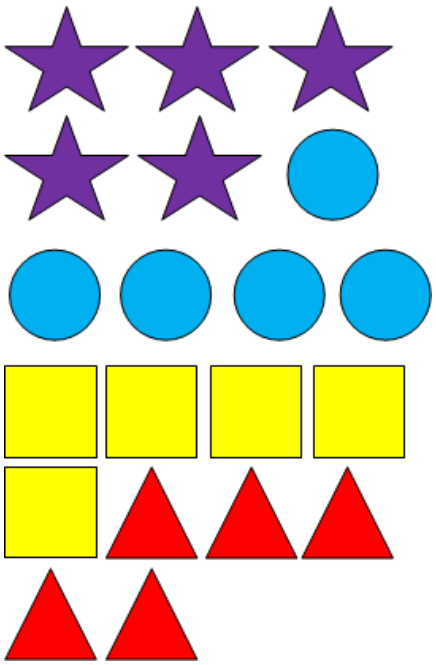


Рисунок 3—Фигуры для распределения команд

После капитанов все участники игры также подходят к педагогу, чтобы вытащить фигуру из пакета (квадрат, треугольник, круг, звездочка), формируются команды, каждая из которых получает маршрутный лист.

Каждая из команд пройдет 5 этапов игры. В маршрутных листах у каждой группы определенный порядок. Правила игры на этапах

объясняют помощники педагога. Общие правила игры озвучивает педагог:

– На каждую станцию приходим с улыбкой и отличным настроением, а также со стремлением победить.

– Запрещено пользоваться телефоном, за это налагается штраф.

– Запрещена нецензурная лексика, за это так же налагается штраф, вычитаются баллы.

Маршрутный лист № 1

Название команды_____

№	Название станции	Баллы	Подпись
1.	Пазлы		
2.	Инфоребусы		
3.	Типы изображений		
4.	Интерфейс MS Excel		
5.	Поиск слов		

Маршрутный лист № 2

Название команды_____

№	Название станции	Баллы	Подпись
1.	Поиск слов		
2.	Пазлы		
3.	Инфоребусы		
4.	Типы изображений		
5.	Интерфейс MS Excel		

Маршрутный лист № 3

Название команды_____

№	Название станции	Баллы	Подпись
1.	Интерфейс MS Excel		
2.	Поиск слов		
3.	Пазлы		
4.	Инфоребусы		
5.	Типы изображений		

Маршрутный лист № 4

Название команды_____

№	Название станции	Баллы	Подпись
1.	Типы изображений		
2.	Интерфейс MS Excel		
3.	Поиск слов		
4.	Пазлы		
5.	Инфоребусы		

Рисунок 4—Маршрутные листы команд

На каждом этапе, после его успешного прохождения, команде будут выдаваться ключи, на обратной стороне которых будут написаны части четверостишия про успех:

«Успех всегда, лишь тех, по жизни ждет

и это безусловно, без сомнения,

не тех, кто раньше утром, всех, встает,

а тех, кто встал — в хорошем настроении!»

Помощник наблюдает за соблюдением правил каждой командой на своём этапе и по итогу выставляет баллы на маршрутных листах.

Таблица 2 — Памятка помощнику «Выставление баллов командам на этапах»

Название этапа	Баллы	Условие
«Пазлы»	2	команда прошла два уровня этапа успешно
	1	команда прошла один уровень этапа
	0	Команда не прошла ни один уровень этапа
«Инфоребусы»	Макс. 8	программа автоматически выдает полученные баллы
«Типы изображений»	2	команда успешно и без ошибок справилась с этапом
	1	команда справилась с этапом с ошибками
«Интерфейс MS Excel»	2	команда успешно и без ошибок справилась с этапом
	1	команда справилась с этапом с ошибками
«Поиск слов»	2	команда успешно справилась с этапом

Максимальное количество набранных баллов - 16.

Всем участникам в каждой команде будет вручена грамота «Лучший знаток информатики» и вручен сладкий приз.

Первый этап «Пазлы»

Та команда, которая пройдёт этапы быстрее и качественнее остальных, соберет из полученных ключей четверостишие в правильном порядке - будет объявлена победителем игры. В случае завершения прохождения этапов игры двух и более команд одновременно, сверяются баллы, выставленные на маршрутном листе помощниками и определяется победитель с наибольшим количеством.

Первый этап «Пазлы». Этап состоит из двух уровней. На первом предлагается собрать картинку в программной оболочке. Дано изображение рабочего окна Microsoft Word.

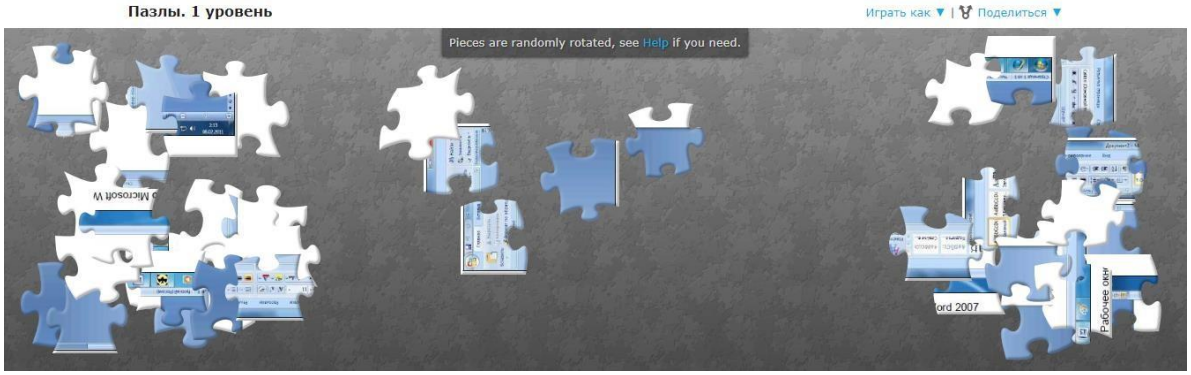


Рисунок 5 — Вид первого уровня этапа «Пазлы»

Задача студентов, удерживая левой кнопкой мыши детали, нужно собрать пазл. Также детали можно переворачивать, удерживая деталь левой кнопкой мыши и щелкая по колесику мыши.

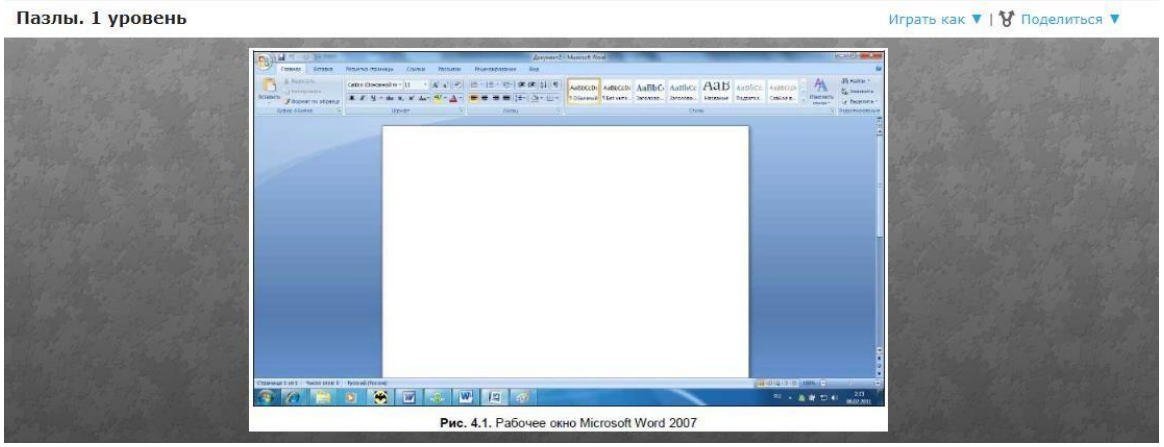


Рисунок 6 — Итоговое собранное изображение первого уровня этапа «Пазлы»

На втором уровне задача участников поставить в соответствие группам форматов, конкретные форматы графических файлов, исходя из изученного материала по теме 1.3. Работа с пакетами прикладных программ обработки отраслевой информации», профессионального модуля ПМ.01 «Обработка отраслевой информации».

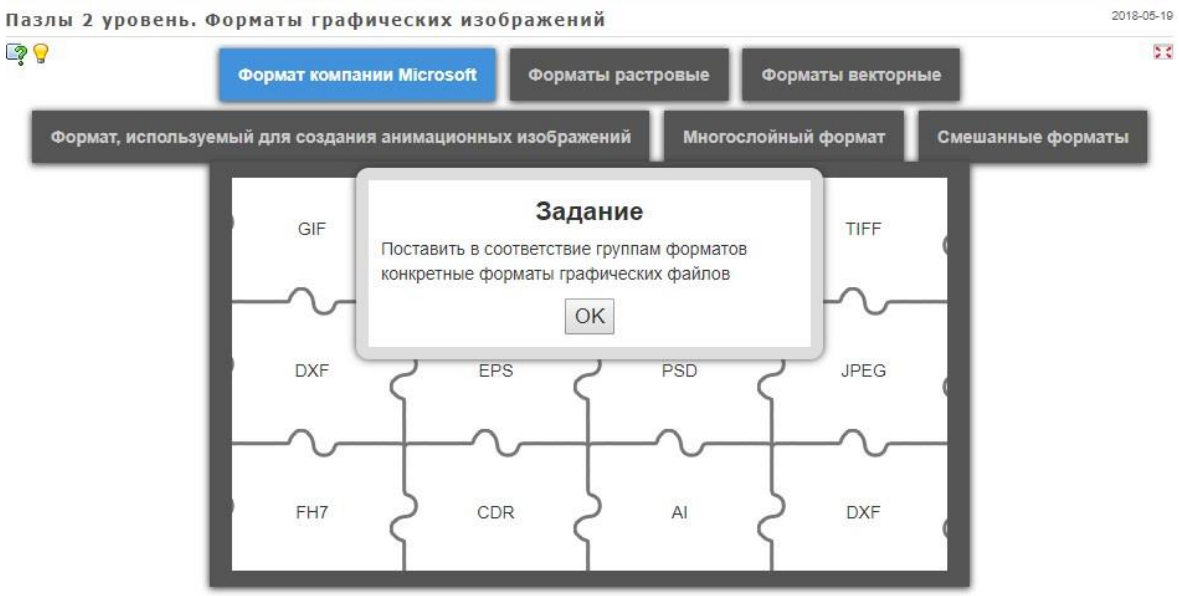


Рисунок 7 — Вид второго уровня этапа «Пазлы»

Выбирая группу форматов, участники щелкают по подходящему «пазлу» и постепенно открывают картинку.

Рисунок 8 — Вид второго уровня этапа «Пазлы»

После успешного прохождения второго уровня помощник выдает ключ, на обратной стороне которого расположена часть фразы из четверостишия про успех. («успех всегда, лишь тех, по жизни ждет»).

Второй этап «Инфоребусы»

Студентам предлагается отгадать ребусы в программной оболочке «Google Формы», где под каждым ребусом нужно вписать полученный ответ. Ответ вписывается на русском языке.

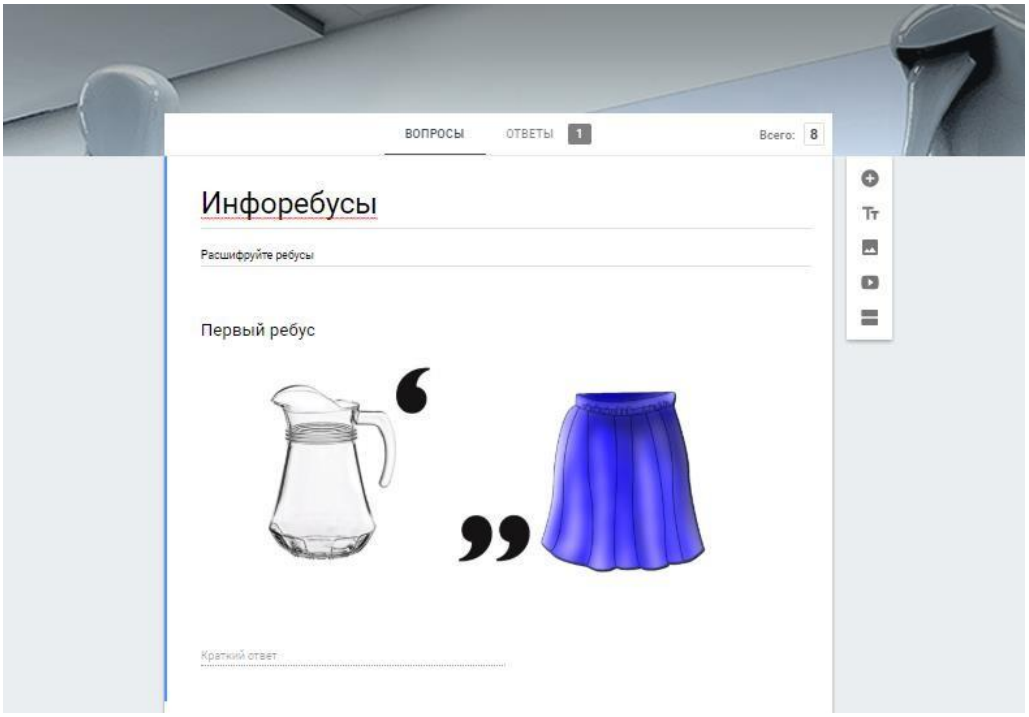


Рисунок 9 — Вид второго этапа «Инфоребусы»

После выполнения теста нажать клавишу «Отправить» и в открывшемся окне нажать «Посмотреть баллы». Помощник вписывает то количество баллов, которое выдаст программа.

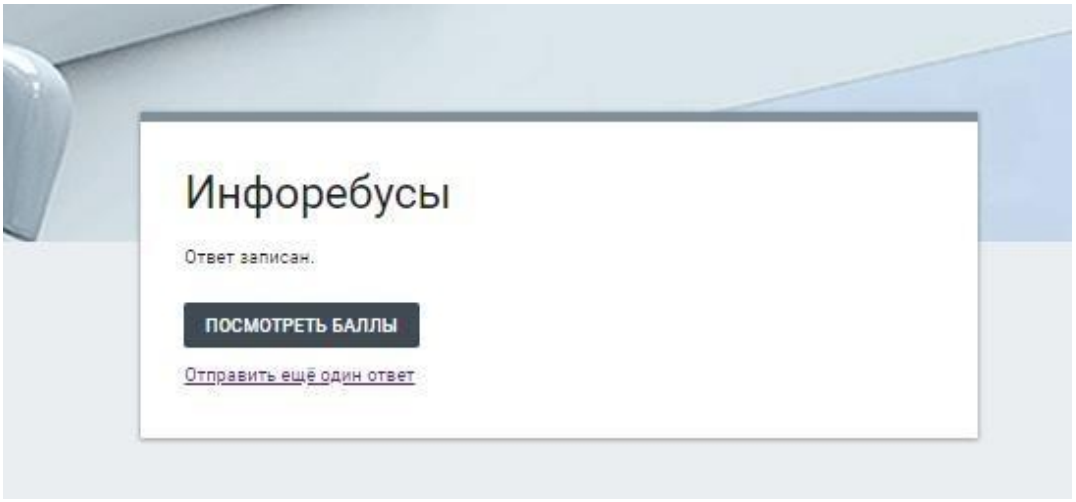


Рисунок 10 — Скриншот после прохождения этапа «Инфоребусы»

Рисунок 11 — Скриншот полученного балла после прохождения этапа «Инфоребусы»

После успешного выполнения задания помощник выдаёт ключ с фразой на обратной стороне («и это, безусловно, без сомнения,»).

Третий этап «Типы изображений».

Обучающиеся определяют к какому виду (растровое или векторное) относятся изображения, данные в игровой разработке. Знания и навыки были получены при изучении темы 3.1 «Теоретические основы компьютерной графики», темы 3.2. «Векторная графика», темы 3.3. «Растровая графика», профессионального модуля ПМ.01 «Обработка отраслевой информации».

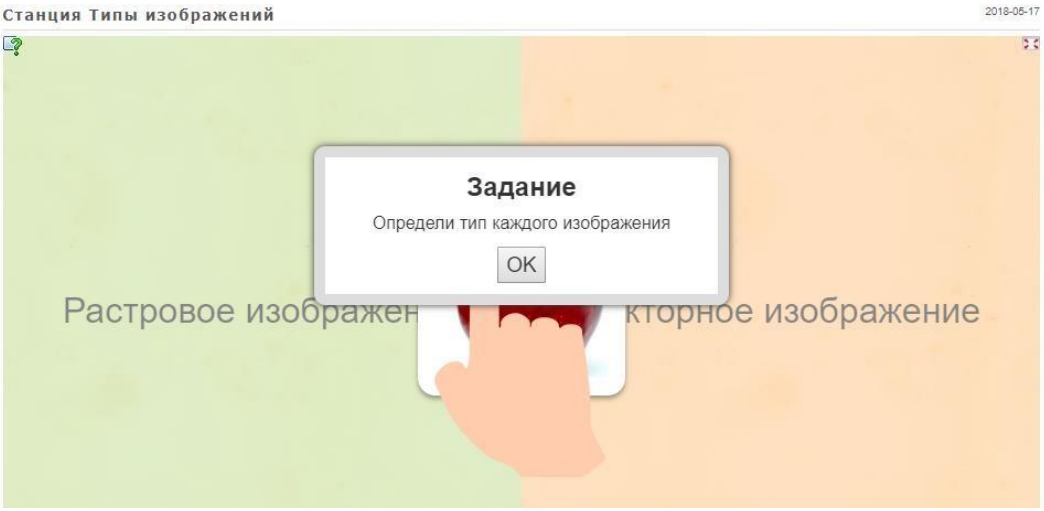


Рисунок 12 —Вид третьего этапа «Типы изображений»

Чтобы перетащить картинки в нужную область, необходимо удерживать левую кнопку мыши на картинке и перетащить в области «растровое изображение» или «векторное изображение»

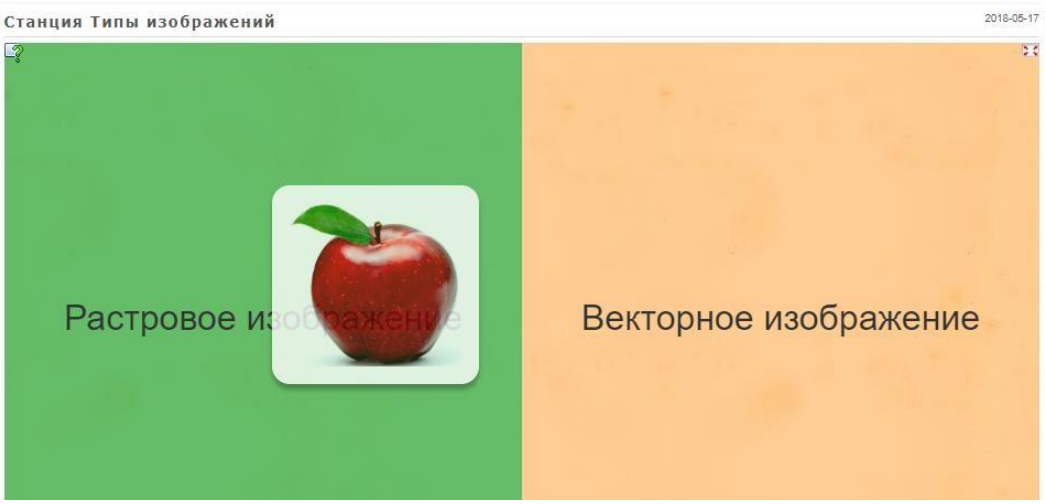


Рисунок 13 —Вид третьего этапа «Типы изображений»

По завершению выдачи изображений программой, необходимо нажать на кнопку «галочка» в правом нижнем углу, после чего программа выдаст результат.

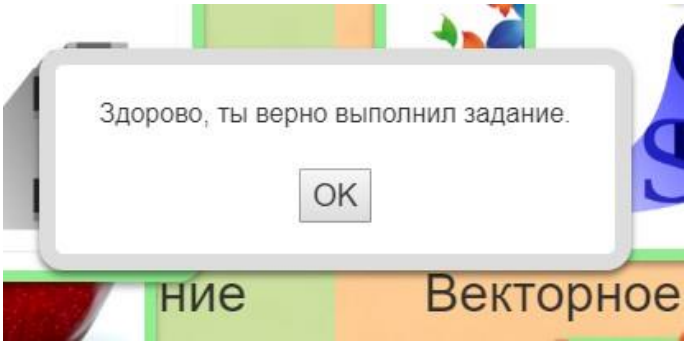


Рисунок 14 — Окно успешного завершения этапа «Типы изображений»

После успешного выполнения задания, помощник ставит балл в маршрутный лист и выдает команде ключ с частью фразы «— в хорошем настроении!»

Четвертый этап «Интерфейс MS Excel».

В программной оболочке представлено окно программы Microsoft Excel с синими указателями.

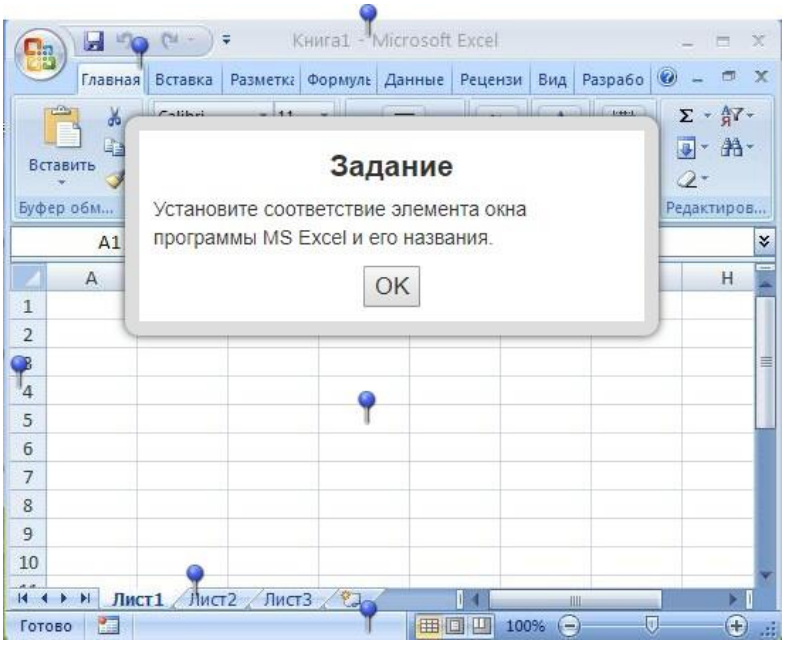


Рисунок 15 — Вид четвертого этапа «Интерфейс MS Excel»

Задача участников - назвать указанные «булавками» части рабочего пространства программы Microsoft Excel, изученного по теме 1.4. «Прикладные программы обеспечения обработки экономической информации», профессионального модуля ПМ.01 «Обработка отраслевой информации». При нажатии левой кнопкой мыши по «булавке», выходит окно с выбором названия данной части.

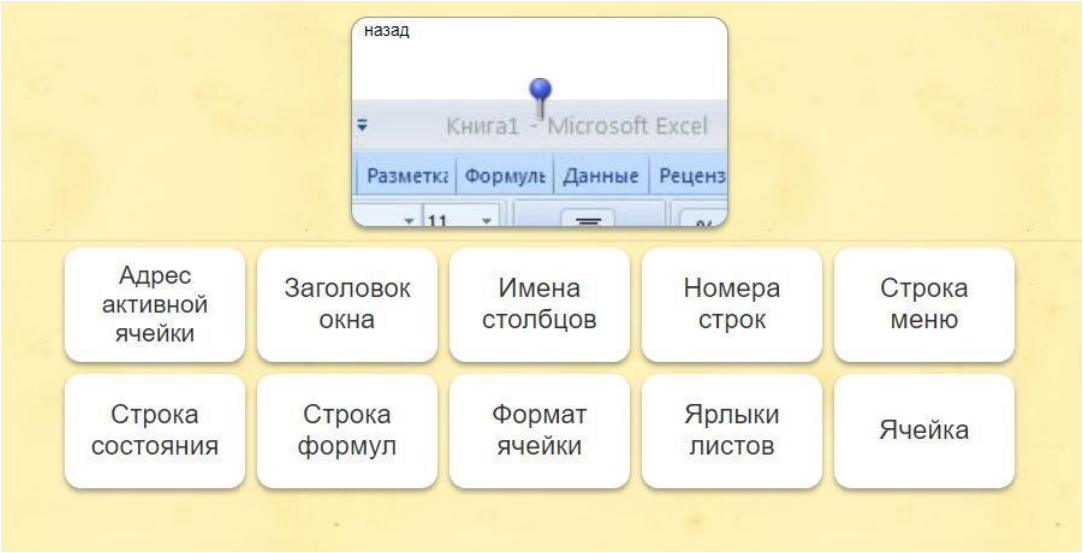
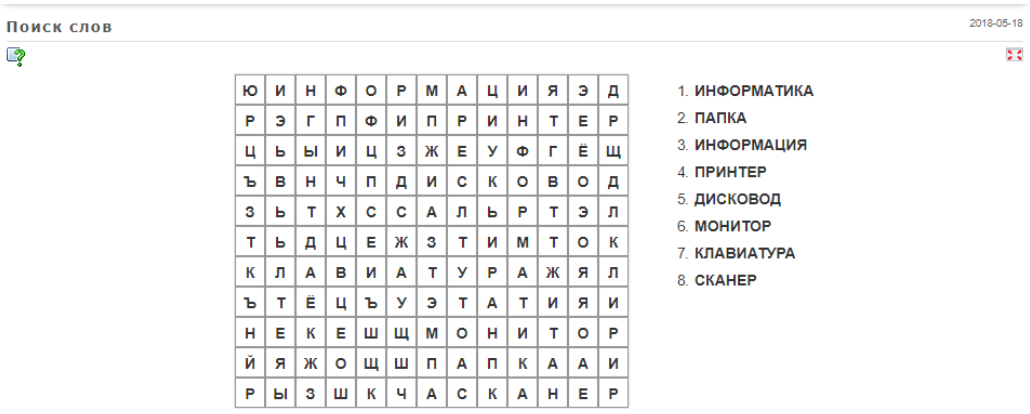


Рисунок 16 — Вид четвертого этапа «Интерфейс MS Excel»

После успешного выполнения задания, помощник выдаёт ключ с частью фразы («не тех, кто раньше утром, всех, встает,»)

Пятый этап «Поиск слов»

Дана таблица с буквами, справа имеется список слов. Задача студентов - отыскать в этой таблице все необходимые слова. Слова расположены только по вертикали или горизонтали. Чтобы выбрать слово нужно удерживать левую кнопку мыши, провести по буквам и собрать слово.



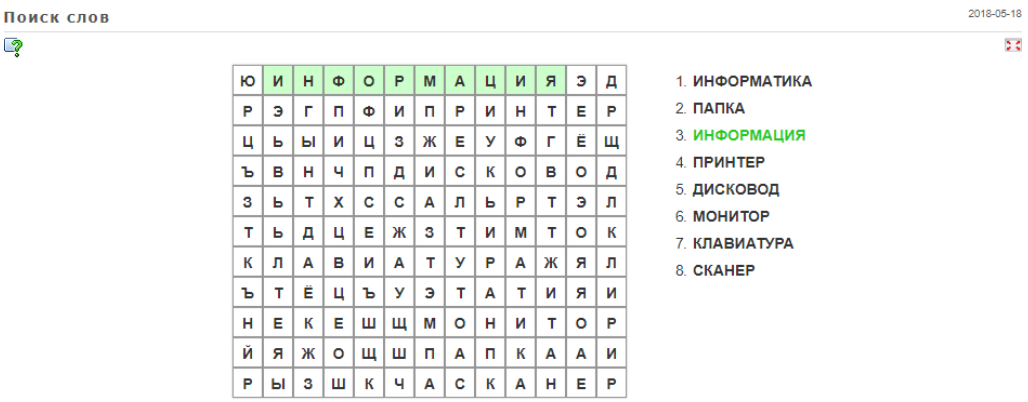


Рисунок 17 —Вид пятого этапа «Поиск слов»

После нахождения всех слов, помощник выдаёт команде ключ, на обратной стороне которого написана фраза («а тех, кто встал»).

Для активизации внимания, интереса, профессиональной заинтересованности в будущей профессии, элементы игровых технологий, а именно, задания, необходимо применять информационно-компьютерные технологии. Разработанные игровые задания являются по своей функции программным педагогическим средством.

Педагогическое программное средство - это целостная дидактическая система, основанная на использовании компьютерных технологий и средств Интернета, ставящая целью, обеспечить обучение по индивидуальным и оптимальным учебным программам с управлением процесса обучения.

Разработка электронного образовательного ресурса к учебно-методическому обучению для организации самостоятельной работы студентов колледжа по профессиональному модулю ПМ.01 «Обработка отраслевой информации» является отдельным и самостоятельным этапом исследования и регламентируется научно-методическими требованиями к разработке педагогических программных средств.

ГЛАВА 2. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЮЖНО-УРАЛЬСКОГО ГОСУДАРСТВЕННОГО КОЛЛЕДЖА

2.1 Понятие политики информационной безопасности, обзор нормативной документации в Российской Федерации

Информационная безопасность остается сегодня важнейшим элементом развития цифровой экономики Российской Федерации. Расширение электронного взаимодействия участников рынка и масштабное использование новых информационных технологий невозможно без глубокой интеграции культуры информационной безопасности во все сферы деятельности коммерческих организаций и государственных структур страны. Политики информационной безопасности (ИБ), будучи наиболее эффективным инструментом по повышению в организациях культуры информационной безопасности, остаются значимым фактором и в современных условиях. Более того, с усилением «цифровизации» процессов экономической деятельности и государственного управления в Российской Федерации роль политик ИБ будет только возрастать.

Политика безопасности — совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации.

Для построения политики информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты информационной системы:

– защита объектов информационной системы;

– защита процессов, процедур и программ обработки информации;

– защита каналов связи;

– подавление побочных электромагнитных излучений;

– управление системой защиты.

При этом, по каждому из перечисленных выше направлений политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:

– определение информационных и технических ресурсов, подлежащих защите;

– выявление полного множества потенциально возможных угроз и каналов утечки информации;

– проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

– определение требований к системе защиты;

– осуществление выбора средств защиты информации и их характеристик;

– внедрение и организация использования выбранных мер, способов и средств защиты;

– осуществление контроля целостности и управление системой защиты.

Политика информационной безопасности оформляется в виде документированных требований на информационную систему. Документы обычно разделяют по уровням описания (детализации) процесса защиты.

Оптимальное и контролируемое обеспечение информационной безопасности (далее – ИБ) требует наличия пакета документов, системно описывающих цели и взаимосвязи процессов по их достижению. Классически такая документация разделяется по уровням, иерархия ее построения визуально представляется в виде пирамиды, демонстрируемой на рисунке 18.

Рисунок 18 - Иерархия документации по информационной безопасности

Стоит отметить, что количество уровней иерархии документации в организации определяется спецификой организации и может быть различно. Наиболее часто встречается 3-х и 4-х уровневая иерархия документации.

Создавать и развивать комплексную систему ИБ необходимо, руководствуясь едиными принципами и подходами. В противном случае, конечный результат может представлять собой разрозненный набор технических средств и организационно-распорядительных документов организации, который нельзя будет назвать «системой» и эффективность которого будет невысока. Потраченные организацией материальные ресурсы не дадут ожидаемого эффекта. Распространена ситуация, когда подразделение ИБ планирует свою деятельность, исходя из исключительно внутреннего понимания бизнес-процессов организации, субъективно определяет актуальные цели и задачи ИБ. При этом стандартно возникают проблемы с обоснованностью целесообразности внедрения той или иной технологии ИБ в организации, с выделением и обоснованностью бюджета на ИБ.

Первый уровень иерархической структуры документации по информационной безопасности. Разработка Концепции или стратегии информационной безопасности (ИБ) нацелена на решение указанных проблем. Концепция / стратегия ИБ должна отражать позицию руководства организации в вопросах обеспечения ИБ и определять цели, задачи и общие принципы, в соответствии с которыми будет строиться комплексная система ИБ. Концепция или стратегия ИБ должна представлять собой высокоуровневый документ, определяющий развитие комплексной системы ИБ в организации на несколько лет вперед.

Концепция / стратегия ИБ, как и любой другой документ, может разрабатываться с различным вниманием к деталям и нуждам конкретной организации. Однако одним из основных требований, которым должны соответствовать такого рода документы, является комплексность, поскольку, если какие-либо нюансы не будут учтены в документе, то они могут быть упущены вовсе.

Поэтому Концепция / стратегия ИБ должна учитывать самые различные моменты:

– требования федерального законодательства, требования законодательства субъекта Российской Федерации, требования регуляторов, отраслевые требования;
– национальные федеральные и целевые программы;
– стандарты ИБ;
– угрозы ИБ, актуальные для данной организации;
– мировые практики;
– современные и перспективные тренды и т. д.

Формальные требования к структуре или оформлению Концепции / стратегии ИБ отсутствуют, но по сложившейся практике Концепция / стратегия ИБ строится согласно логике «объект защиты –

угрозы – меры защиты» и основывается на лучших практиках, в т. ч. мировых. В общем случае Концепция / стратегия ИБ содержит:

- основные цели и задачи ИБ;
- основные принципы обеспечения ИБ;
- описание объекта защиты;
- верхнеуровневую модель угроз и нарушителя безопасности информации;
- описание общих методов обеспечения ИБ;
- принципы управления ИБ;
- описание организации работ по обеспечению ИБ (состав мероприятий);
- меры обеспечения ИБ;
- разделение ответственности и порядок взаимодействия;
- принципы оценки и контроля;
- нормативно-методическое обеспечение;
- механизм реализации Концепции / стратегии ИБ;
- ожидаемый эффект.

Особо отметим, что типовых Концепций / стратегий ИБ не существует. Концепция / стратегия ИБ – исключительно практический документ, максимально соответствующий нуждам конкретной организации.

Для построения архитектуры комплексной системы ИБ необходимо осуществить ряд взаимосвязанных действий, объединенных единым стратегическим замыслом и представленных в структурированном виде. Процесс разработки Концепции / стратегии ИБ отражен на рисунке 19.

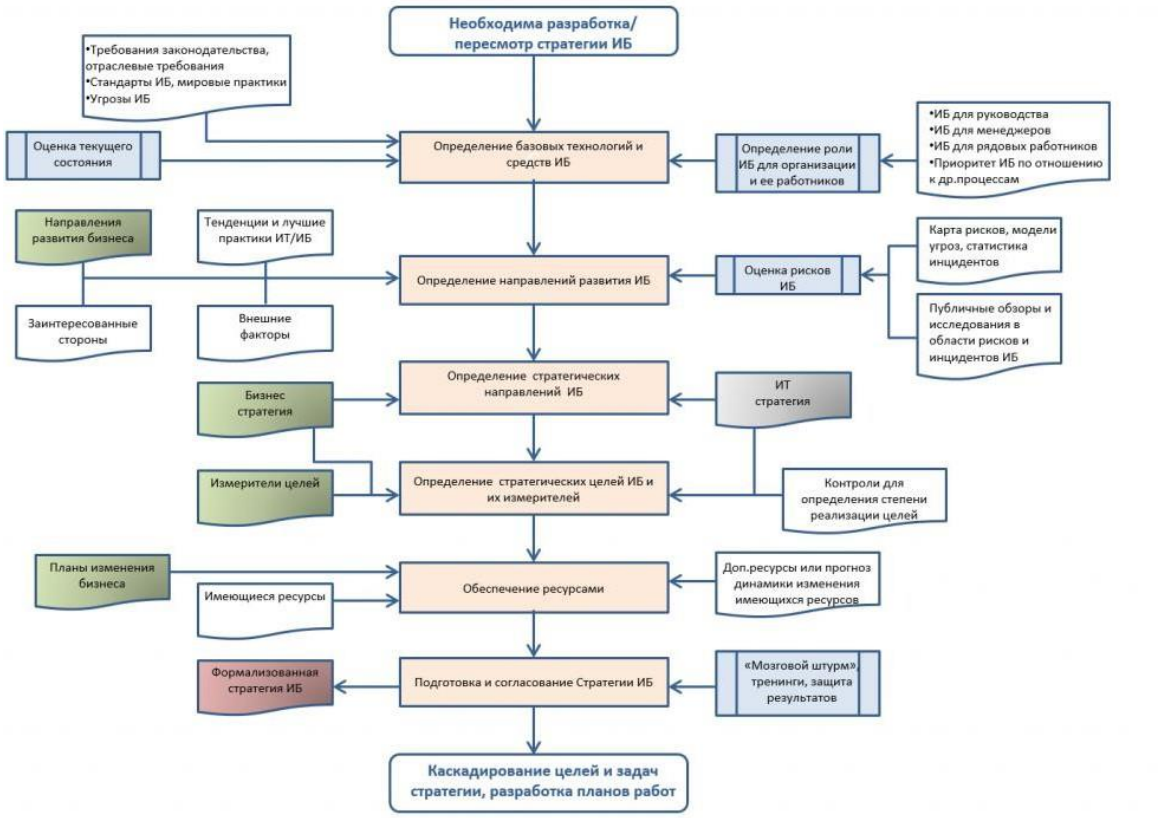


Рисунок 19 - Процесс разработки Концепции / стратегии ИБ

В случаях, когда организации ограничиваются разработкой политики ИБ, следует исходить из того, что политика ИБ становится основным высокоуровневым документом организации, определяющим подходы, методики достижения целей ИБ через постановку стратегических целей, формирующим подходы к построению моделей угроз и атак, а также методики выявления, оценки и прогнозирования рисков ИБ. Наиболее полно требования к форме, содержанию и задачам политики ИБ сформированы в банковской сфере [12]-[14]. Так же можно отметить идентичность политик ИБ органов государственной власти [15]-[16] или органов здравоохранения [17]-[18], в силу серьезного централизованного ведомственного и отраслевого регулирования сферы их деятельности. Для коммерческих организаций характерна более узкая направленность политики ИБ на обеспечение безопасности персональных данных в организации [19]-[20].

Наиболее существенное влияние на состав и содержание разделов политики ИБ организации оказывает актуализация законодательства Российской Федерации и Евразийского экономического союза [21].

Так, в 2006 году с целью регулирования отношений, связанных с обработкой персональных данных (далее – ПДн), были внесены изменения в законодательство Российской Федерации [22]. Мерами, направленными на обеспечение выполнения оператором обязанностей, определенных российским законодательством, предусмотрена обязательная разработка и утверждение в каждой организации политики обработки персональных данных [23]. Разработка данной политики невозможна без интеграции технических и организационных средств защиты ПДн в комплексную систему ИБ организации.

Внесение отдельного состава административного правонарушения за нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, заставило организации перейти от формального исполнения требований российского законодательства в виде утверждения типового пакета документации по ИБ к организации реальных процессов обеспечения и управления ИБ [24].

В дальнейшем были законодательно урегулированы отношения, связанные с обработкой государственного информационного ресурса в государственных информационных системах [25].

Возросшая степень автоматизации и информатизации объектов критической информационной инфраструктуры Российской Федерации привела в 2016 году к необходимости выделения вопросов обеспечения безопасности критической информационной инфраструктуры в отдельную область законодательства [26].

Выполнение требований по защите ПДн, установленных нормативными правовыми актами Российской Федерации, приводит к необходимости формирования многоуровневой экономически обоснованной комплексной системы ИБ в организации.

Обеспечение безопасности ПДн достигается:

– определением угроз безопасности ПДн при их обработке в информационной системе персональных данных (далее – ИСПДн);

– применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

– учетом машинных носителей ПДн;

– обнаружением фактов несанкционированного доступа к ПДн;

– восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

– контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности ПДн в ИСПДн [27].

Второй уровень иерархической структуры документации по информационной безопасности. На втором уровне иерархии документации по обеспечению ИБ находятся документы, определяющие правила, требования и принципы, используемые применительно к отдельным областям ИБ, видам и технологиям деятельности

организации – частные политики ИБ. Кроме того, в состав документов данного уровня рекомендуется включить стандарты технологий обеспечения ИБ организации [28].

Для обеспечения взаимодействия направлений ИБ не рекомендуется повторение одинаковых правил и (или) требований в различных частных политиках ИБ. Включение в частную политику ИБ правила и (или) требования, содержащегося в другой частной политике ИБ, целесообразно осуществлять посредством соответствующей ссылки.

Частные политики ИБ формируются на основании принципов, требований и задач, определенных в Концепции / стратегии ИБ организации, с учетом детализации, уточнения и дополнительной классификации информационных активов и угроз, определения владельцев информационных активов, анализа, оценки рисков и возможных последствий реализаций угроз ИБ в границах области действия регламентируемой области ИБ или технологии.

Базовый набор частных политик ИБ. Комплектность частных политик ИБ определяется исходя из используемых в организации информационных технологий, технических и организационных мер ИБ – элементов комплексной системы ИБ. Базовый набор элементов комплексной системы ИБ приведен на рисунке 20.

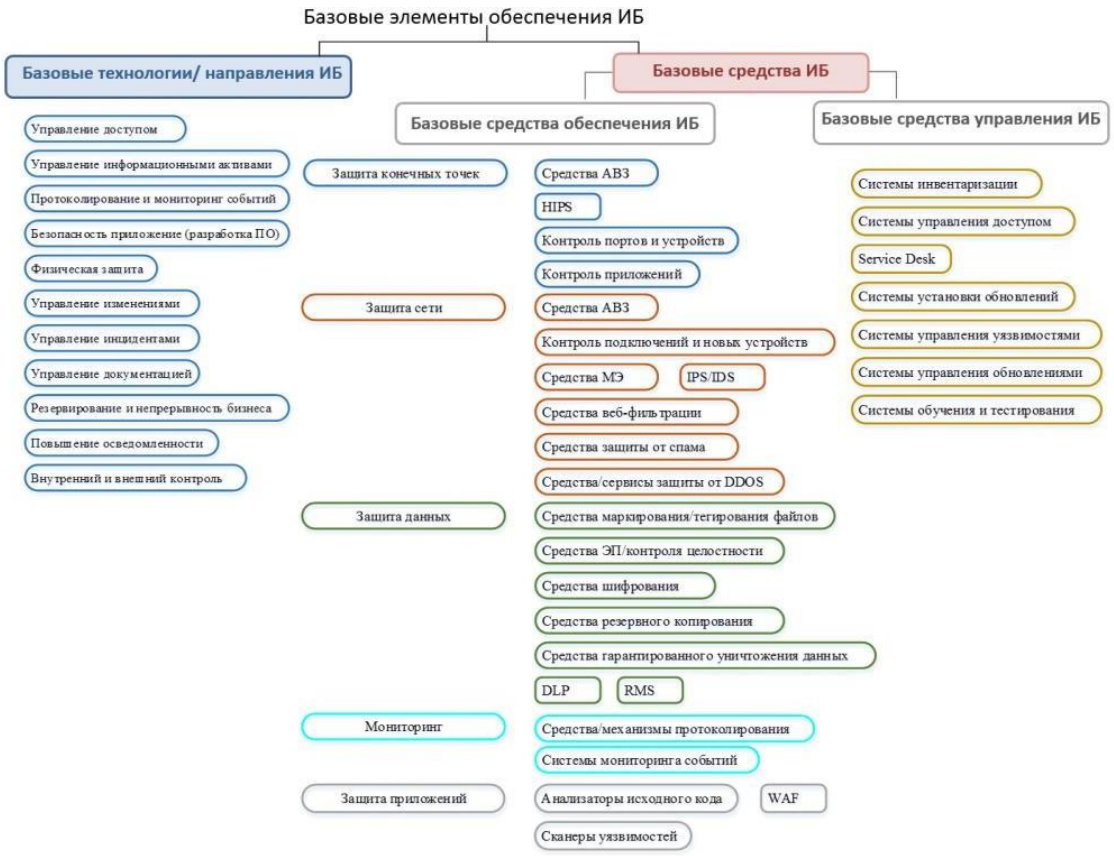


Рисунок 20 - Базовый набор элементов комплексной системы ИБ

Проверка качества частной политики ИБ. В частные политики ИБ образовательной организации рекомендуется включать положения, определяющие:

1. Цели и задачи ИБ, на обеспечение которых направлена частная политика.

2. Область действия политики ИБ, определение объектов (активов) защиты, уязвимостей, угроз и оценка рисков, связанных с объектами защиты.

3. Сведения о виде деятельности, на обеспечение ИБ которой направлено действие положений частной политики; о совокупности информационных технологий, применяемых в рамках выполнения данного вида деятельности; об основных технологических процессах, реализующих указанные технологии.

4. Определение субъектов (ролей), на которых распространяется действие документа. В качестве субъектов (ролей) могут

рассматриваться как структурные подразделения организации, так и отдельные исполнители.

5. Содержательную часть документа (требования и правила).

6. Обязанности по обеспечению ИБ в рамках области действия частной политики ИБ, описание функций субъектов (ролей) над управляемыми объектами в рамках регламентируемых технологических процессов.

7. Положения по контролю реализации частной политики ИБ.

8. Ответственность за реализацию и поддержку документа.

9. Условия пересмотра документа [12].

В силу высокой изменчивости информационных технологий, технологий обеспечения ИБ и появления новых средств ИБ, а также с ростом возможностей нарушителя ИБ, рекомендуется установить период актуализации частных политик ИБ в один год.

Для проверки полноты разработанных частных политик ИБ желательно составлять контрольные листы.

*Управление доступом. У*правление доступом к защищаемым информационным ресурсам организации — наиболее существенная функция, реализуемая комплексной системой ИБ организации. Без реализации процесса управления доступом к информационным ресурсам организации невозможно обеспечить защиту от несанкционированного доступа к ним.

Риски для информации и средств обработки информации организации, являющиеся следствием бизнес-процессов, в которых участвуют сторонние организации, необходимо определять и реализовывать соответствующие меры и средства контроля и управления прежде, чем будет предоставлен доступ [29].

При необходимости разрешения доступа сторонней организации к средствам обработки информации или к защищаемым информационным ресурсам организации следует проводить оценку рисков ИБ для

актуализации существующих мер контроля и управления ИБ в организации.

Доступ сторонних организаций к защищаемым информационным ресурсам организации не должен предоставляться до реализации соответствующих мер и до подписания соглашения, определяющего сроки и условия подключения или доступа к защищаемым информационным ресурсам.

Необходимо предусмотреть осведомленность сторонних организаций об исполнении надлежащим образом требований ИБ, а также убедиться в юридическом закреплении ответственности и обязательств сторонних организаций в отношении доступа, обработки, передачи или иных действий с защищаемыми информационными ресурсами организации.

Если управление ИБ осуществляется в рамках договоров аутсорсинга, то в договорах должно быть оговорено, каким образом третья сторона будет гарантировать поддержание адекватного уровня ИБ организации, определенный оценкой риска, а также адаптацию к выявленным рискам и изменениям рисков.

Некоторые из различий между аутсорсингом и другими формами обеспечения услуг третьими сторонами включают в себя вопросы ответственности, планирование переходного периода и возможного срыва операций в течение данного периода, планирование мероприятий на случай непредвиденных ситуаций и тщательность проверок, а также сбор и управление информацией по инцидентам ИБ. Поэтому важно, чтобы организация планировала и управляла переходом к договорам аутсорсинга и применяла соответствующий процесс управления изменениями и перезаключения договоров либо окончания действия договоров. В договоре необходимо учитывать процедуры непрерывной обработки на случай, если третья сторона окажется неспособной

поставлять свои услуги, для предотвращения какой-либо задержки по организации замены услуг.

Управление инцидентами ИБ. Одним из важных процессов в комплексной системе ИБ организации является процесс управления инцидентами ИБ. Наличие корректной политики управления инцидентами ИБ и функционирующий на ее основе процесс управления инцидентами ИБ позволяют поддерживать комплексную систему ИБ в актуальном состоянии (проводить мероприятия по совершенствованию комплексной системы ИБ), корректируя как набор мероприятий по обеспечению ИБ, так и внося изменения в планирование мероприятий ИБ в организации.

Основными целями процесса управления инцидентами ИБ являются минимизация потерь организации, вызванных инцидентами ИБ, и снижение риска возникновения повторных инцидентов ИБ за счет обеспечения оперативности выявления инцидентов ИБ и реализации эффективного управления разрешением инцидентов ИБ. Выявление событий ИБ в масштабе реального времени и их правильная классификация как инцидентов ИБ позволяет организации существенно снизить материальные и репутационные потери от компьютерных атак, а также понизить издержки от «ложных срабатываний» комплексной системы ИБ. Оптимизируется состав сил и средств организации, назначаемых на ликвидацию последствий инцидентов ИБ.

К основным задачам процесса управления инцидентами ИБ относятся:

– быстрое обнаружение инцидентов ИБ;

– обеспечение эффективного разрешения инцидентов ИБ;

– координация реагирования на инциденты ИБ и информирование в установленные нормативными документами сроки заинтересованных внешних организаций;

– минимизация нарушений порядка работы и повреждения данных ИС организации, восстановление в кратчайшие сроки работоспособности информационных систем организации при их нарушении в результате инцидента ИБ;

– обеспечение получения достоверной и полной информации о нарушениях ИБ в организации;

– обеспечение сохранности и целостности доказательств возникновения инцидента ИБ, создание условий для накопления и хранения точной информации об имевших место инцидентах ИБ, о рекомендациях;

– обучение персонала организации действиям по обнаружению, устранению последствий и предотвращению инцидентов ИБ.

Как правило, политика управления инцидентами ИБ включает описание целей и задачей процесса; состава событий ИБ и критериев классификации событий ИБ как инцидентов ИБ; стадий процесса управления инцидентами ИБ, ролей работников, задействованных на стадиях процесса управления инцидентами ИБ; организационной структуры процесса управления инцидентами ИБ.

Построение архитектуры системы обеспечения ИБ образовательной организации должно базироваться на соблюдении следующих основных принципов обеспечения ИБ:

1. Простота архитектуры, минимизация и упрощение связей между компонентами, унификация и упрощение компонентов, использование минимального числа протоколов сетевого взаимодействия. Система должна содержать лишь те компоненты и связи, которые необходимы для ее функционирования (с учетом требований надежности и перспективного развития).

2. Апробированность решений, ориентация на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

3. Построение системы из компонентов, обладающих высокой надежностью, готовностью и обслуживаемостью.

4. Управляемость, возможность сбора регистрационной информации обо всех компонентах и процессах, наличие средств раннего выявления нарушений информационной безопасности, нештатной работы аппаратуры, программ и пользователей.

5. Простота эксплуатации, автоматизация максимального числа действий администраторов сети.

6. Эшелонированность обороны – для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

7. Непрерывность защиты в пространстве и времени, невозможность обхода защитных средств – системы должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом принимаются меры по недопущению перехода систем в незащищенное состояние.

8. Равнопрочность обороны по всем направлениям – осуществляется регламентацией и документированием всех способов доступа к ресурсам локальной сети учебного учреждения. В соответствии с этим принципом запрещается создавать несанкционированные подключения к локальной сети учебного учреждения и другими способами нарушать установленный порядок предоставления доступа к информационным ресурсам, который определяется «Политикой управления доступом к ресурсам локальной сети учебного учреждения», «Политикой обеспечения ИБ при взаимодействии с сетью Интернет» и «Политикой обеспечения ИБ

удаленного доступа к ресурсам локальной сети учебного учреждения Образовательного учреждения».

9. Профилактика нарушений безопасности – в большинстве случаев для Образовательного учреждения экономически оправданным является принятие предупредительных мер по недопущению нарушений безопасности в отличие от мер по реагированию на инциденты, связанных с принятием рисков осуществления угроз информационной безопасности. Однако это не исключает необходимости принятия мер по реагированию на инциденты и восстановлению поврежденных информационных ресурсов. В соответствии с данным принципом должен проводиться анализ рисков, опирающийся на модель угроз безопасности и модель нарушителя, определяемые настоящей Концепцией. Многие риски можно уменьшить путем принятия превентивных мер защиты.

10. Минимизация привилегий - политика безопасности должна строиться на основе принципа «все, что не разрешено, запрещено». Права субъектов должны быть минимально достаточными для выполнения ими своих служебных обязанностей;

11. Разделение обязанностей между администраторами локальной сети учебного учреждения определяется должностными инструкциями и регламентами администрирования.

12. Экономическая целесообразность. Обеспечение соответствия ценности информационных ресурсов Образовательного учреждения и величины возможного ущерба (от их разглашения, утраты, утечки, уничтожения и искажения) уровню затрат на обеспечение информационной безопасности. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать экономические показатели работы автоматизированных систем Образовательного учреждения, в которых эта информация циркулирует.

13. Преемственность и непрерывность совершенствования. Обеспечение постоянного совершенствования мер и средств защиты информационных ресурсов и информационной инфраструктуры на основе преемственности организационных и технических решений, кадрового аппарата, анализа функционирования систем защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по ее защите, достигнутого передового отечественного и зарубежного опыта в этой области. При выборе программно-технических решений по обеспечению ИБ Образовательного учреждения, предпочтение отдается решениям, обеспечивающим соблюдение основных принципов ИБ, а также удовлетворяющих следующим критериям:

1. Поддержка международных, национальных, промышленных и Интернет стандартов (предпочтение отдается международным стандартам).

2. Поддержка наибольшей степени интеграции с корпоративными программно-аппаратными платформами и используемыми СЗИ;

3. Унификация разработчиков и поставщиков используемых продуктов.

4. Унификация средств и интерфейсов управления подсистемами ИБ.

Организация работ по защите информации. Организация и проведение работ по обеспечению ИБ образовательной организации определяются настоящей концепцией, действующими государственными и международными стандартами и другими нормативными и методическими документами.

Организация работ по обеспечению ИБ возлагается на заместителя директора по информатизации, осуществляющего эксплуатацию и сопровождение ИС, а методическое руководство и контроль над эффективностью предусмотренных мер защиты информации – на

заведущего отделом информационной безопасности Образовательного учреждения.

Эксплуатация ИС Образовательного учреждения осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией, с учетом требований и положений, изложенных в соответствующих разделах настоящего документа.

Комплекс мер по защите информации на предприятии включает в себя следующие мероприятия:

1. Назначение ролей и распределение ответственности за использование информационных ресурсов локальной сети учебного учреждения.
2. Разработка, реализация, внедрение и контроль исполнения планов мероприятий, политик безопасности и других документов по обеспечению ИБ.
3. Подготовка пользователей и технических специалистов к решению проблем, связанных с обеспечением ИБ.
4. Проектирование, развертывание и совершенствование технической инфраструктуры СОИБ.
5. Аудит состояния ИБ Образовательного учреждения.
6. Техническая инфраструктура СОИБ предназначена для решения следующих задач:
7. Защиты внешнего периметра локальной сети учебного учреждения Образовательного учреждения от угроз со стороны внешних сетей за счет использования межсетевого экранирования, контроля удаленного доступа и мониторинга информационных взаимодействий.
8. Защиты серверов образовательного учреждения за счет использования механизмов управления доступом к серверам баз данных, файловым, информационным и почтовым серверам, регистрации и учета событий, связанных с осуществлением доступа к ресурсам серверов

образовательного учреждения, механизмов мониторинга и аудита безопасности.

9. Комплексной антивирусной защиты систем, входящих в состав локальной сети учебного учреждения за счет распределения антивирусных средств (антивирусных сканеров, резидентных антивирусных мониторов и файловых ревизоров) по следующим уровням:

10. Защиты внешнего шлюза в сеть Интернет.

11. Защиты корпоративных серверов.

12. Защиты рабочих мест пользователей.

13. Мониторинга сетевого трафика в реальном масштабе времени с целью выявления злоумышленных действий пользователей локальной сети учебного учреждения и попыток осуществления НСД к ресурсам локальной сети учебного учреждения со стороны внешних злоумышленников.

14. Защиты прикладных подсистем, функционирующих в составе локальной сети учебного учреждения, обеспечение доступности предоставляемых ими прикладных сервисов.

15. Защиты межсетевых взаимодействий между сегментами ИС образовательной организации.

В настоящее время законодательство Российской Федерации активно развивается в целях нормативного и методического обеспечения централизованного сбора информации об инцидентах ИБ, с дальнейшими скоординированными в масштабах всей страны действиями по предотвращению компьютерных атак и ликвидации их последствий. Вопросы оперативного выявления и своевременного реагирования на инциденты ИБ в организации стали вопросами государственной важности и влияют на безопасность Российской Федерации.

Основные нормативные правовые акты в сфере персональных данных:

1. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных».

3. Федеральный закон от 21.07.2014 г. №242 «..«о запрете хранения ПДн россиян заграницей» (вступилвсилу01.09.2015г).

4. Постановление Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5. Постановление Правительства РФ от 15.09.2008 г. №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6. Постановление Правительства РФ от 21.03.2012 г №211. «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

7. Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных (Приказ Роскомнадзора от 11.11.2011 №312).

8. Приказ Роскомнадзора от 19.08.2011г. №706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».

9. Приказ Минкомсвязи от 28.08.2015 №315 «О внесении изменений в Административный регламент Роскомнадзора…» «…О месте нахождения базы данных информации, содержащей персональные данные».

10. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСТЭК РФ от 15.02.2008).

11. Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (Приказ ФСТЭК РФ от 14.02.2008 г.).

12. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

13. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. №17 «Требования о защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах».

14. Методический документ**.** Меры защиты информации в государственных информационных системах. (Утверждено ФСТЭК России 11.02.2014г.).

15. Банк данных угроз безопасности информации. (Утверждено ФСТЭК России 06.03.2015 №240/22/879).

16. Приказ Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите

персональных данных для каждого из уровней защищенности (Приказ ФСБ РФ от 10.07.2014 г. №378).

Нормативные правовые акты, регламентирующие размещение персональных данных на сайте образовательной организации:

- ФЗ от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;

- ПП от 10.07.2013 №582 «Об утверждении Правил размещения на официальном сайте образовательной организации в сети «Интернет» и обновления информации об образовательной организации»;

- Приказ Минобрнауки от 29.05.2014 №785 «Об утверждении требований к структуре официального сайта образовательной организации в сети «Интернет» и формату представления на нем информации»;

- Письмо Рособрнадзора от 25.03.2015 №07-675 с «Методическими рекомендациями представления информации об образовательной организации в открытых источниках с учетом соблюдения требований законодательства в сфере образования»;

- Приказ Роскомнадзора от 05.09.2013 №996 «Об утверждении требований и методов по обезличиванию персональных данных»;

- Методические рекомендации Роскомнадзора от 14.12.2012 «Разъяснение вопросов, касающиеся обработки персональных данных работников, соискателей и лиц, находящихся в кадровом резерве».

Документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.

Оценивая законодательную базу, следует обратить внимание, что к объектам информационной безопасности в Минобрнауки России, региональных министерствах (департаментах) образования,

муниципальных органах управления образованием и в образовательных организациях относят:

- сведения, составляющие государственную тайну, в соответствии с выписками из перечня сведений, подлежащих засекречиванию в министерствах, ведомствах и организациях;
- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информацию, защита которой предусмотрена законодательными актами РФ, в т.ч. и персональные данные;
- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

2.2 Реализация политики информационной безопасности в ГБПОУ «Южно-Уральский государственный колледж»

Базой исследования стал ГБПОУ «Южно-Уральский государственный колледж», располагающийся по адресу: г. Челябинск ул. Курчатова, 7.

Главная цель и направление деятельности ГБПОУ «Южно-Уральский государственный колледж» – повышение качества знаний и уровня профессиональных компетенций выпускников колледжа за счет разработки, создания и внедрения инновационных образовательных технологий, основанных на E-Learning, электронных учебно-методических комплексах, компетентностном подходе. Данные технологии и формы обучения позволили реально повысить качество профессиональной подготовки, прежде всего практического обучения, и сделали выпускников колледжа востребованными на рынке труда [26].

В колледже ведется целенаправленная работа по созданию и развитию современных технологий обучения с привлечением системы электронного обучения E-Learning, формированию новых программ подготовки выпускников различных уровней в соответствии с требованиями рынка, открытию новых специальностей и специализаций по направлениям в соответствии с требованиями промышленности, сферы торговли и услуг, разработки и осуществления систем дополнительного, дистанционного и непрерывного образования, внедрения системы трудоустройства выпускников на базе длительного взаимодействия колледжа и потребителей (предприятий, фирм и организаций) при подготовке специалистов различного уровня и профиля.

Рассмотрим меры обеспечения информационной безопасности в ГБПОУ «Южно-Уральский государственный колледж».

Меры обеспечения информационной безопасности организационного уровня. Система обеспечения ИБ реализуется путем сочетания мер организационного и программно-технического уровней. Организационные меры состоят из мер административного уровня и процедурных мер защиты информации. Основой мер административного уровня, то есть мер, предпринимаемых руководством Образовательного учреждения, является политика информационной безопасности. Под политикой информационной безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию колледжа в области ИБ, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Политика безопасности колледжа определяется настоящим документом, а также другими нормативными и организационно-

распорядительными документами образовательной организации, разрабатываемыми на основе настоящей концепции. К числу таких документов относятся следующие:

1. Политика защиты от НСД к информации.
2. Политика предоставления доступа пользователей в ИС.
3. Политика управления паролями.
4. Политика восстановления работоспособности АС в случае аварии.
5. Политика резервного копирования и восстановления данных.
6. Политика предоставления доступа к ресурсам сети Интернет.
7. Политика управления доступом к информационным ресурсам ИС Образовательного учреждения.
8. Политика внесений изменений в программное обеспечение.
9. Политика управления доступом к АРМ Пользователя.
10. Политика использования электронной почты.
11. Политика анализа защищенности ИС Образовательного учреждения.
12. Программа, методика и регламенты тестирования функций СЗИ от НСД к информации.
13. Инструкция, определяющая порядок и правила регистрации распечатываемых документов, содержащих информацию ограниченного доступа, в соответствии с перечнем информации, составляющей информацию ограниченного доступа.
14. Должностные инструкции для операторов, администраторов и инженеров, осуществляющих эксплуатацию и обслуживание ИС Образовательного учреждения.
15. Инструкции для операторов, администраторов и инженеров по обеспечению режима информационной безопасности.

16. Документированная процедура контроля целостности программной и информационной частей ИС Образовательного учреждения.

Меры обеспечения информационной безопасности процедурного уровня. К процедурному уровню относятся меры безопасности, реализуемые сотрудниками образовательной организации. Выделяются следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

В рамках управления персоналом для каждой должности должны существовать квалификационные требования по информационной безопасности. В должностные инструкции должны входить разделы, касающиеся защиты информации. Каждого сотрудника образовательной организации необходимо обучить мерам обеспечения информационной безопасности теоретически и отработать выполнение этих мер практически.

Информационная безопасность ИС образовательной организации зависит от окружения, в котором она работает. Необходимо принять меры для обеспечения физической защиты зданий и прилегающей территории, поддерживающей инфраструктуры и самих компьютеров.

При разработке проекта СОИБ предполагается адекватная реализация мер физической защиты зданий и других помещений, принадлежащих образовательной организации, по следующим направлениям:

- физическое управление доступом;
- противопожарные меры;

– защита поддерживающей инфраструктуры.

Предполагается также адекватная реализация следующих направлений поддержания работоспособности:

– поддержка пользователей ИС;
– поддержка программного обеспечения;
– конфигурационное управление;
– резервное копирование;
– управление носителями;
– документирование;
– регламентные работы.

Программа информационной безопасности должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима информационной безопасности преследует две главные цели:

– блокирование нарушителя и уменьшение наносимого вреда;
– недопущение повторных нарушений.

Механизмы контроля, существенные для образовательной организации с юридической точки зрения, включают в себя:

– защиту данных и тайну персональной информации;
– охрану документов организации;
– права на интеллектуальную собственность.

В соответствии с международным стандартом ISO 17799, а также руководящими документами ФСТЭК, ключевыми также являются следующие механизмы контроля:

1. Политика информационной безопасности.

2. Распределение ролей и ответственности за обеспечение информационной безопасности.

3. Обучение и тренинги по информационной безопасности.

4. Информирование об инцидентах безопасности.

Меры обеспечения информационной безопасности программно-технического уровня

Программно-технические средства защиты располагаются на следующих рубежах:

1. Защита внутренних сетевых сервисов и информационных обменов.

2. Защита серверов и рабочих станций.

3. Защита системных ресурсов и локальных приложений на серверах и рабочих станциях.

На программно-техническом уровне выполнение защитных функций ИС осуществляется следующими служебными сервисами обеспечения информационной безопасности:

– идентификация/аутентификация пользователей ИС;

– разграничение доступа объектов и субъектов информационного обмена;

– протоколирование/аудит действий легальных пользователей;

– экранирование информационных потоков и ресурсов ЛСПД;

– туннелирование информационных потоков;

– шифрование информационных потоков, критической информации;

– контроль целостности;

– контроль защищенности;

– управление СОИБ.

На внешнем рубеже информационного обмена располагаются средства выявления злоумышленной активности и контроля защищенности. Далее идут межсетевые экраны, защищающие внешние

подключения. Они, вместе со средствами поддержки виртуальных частных сетей, объединяемых с межсетевыми экранами, образуют внешний периметр информационной безопасности, отделяющий информационную систему образовательной организации от внешнего мира.

Сервис активного аудита СОИБ (как и управление) должен присутствовать во всех критически важных компонентах и, в частности, в защитных. Это позволит быстро обнаружить атаку, даже, если по каким-либо причинам, она окажется успешной. Управление доступом также должно присутствовать на всех сервисах, функционально полезных и инфраструктурных. Доступу пользователя к ИС образовательной организации должна предшествовать идентификация и аутентификация субъектов информационного обмена (пользователей и процессов).

Средства шифрования и контроля целостности информации, передаваемой по каналам связи, целесообразно выносить на специальные шлюзы, где им может быть обеспечено квалифицированное администрирование.

Последний рубеж образуют средства пассивного аудита, помогающие оценить последствия реализации угроз информационной безопасности, найти виновного, выяснить, почему успех атаки стал возможным.

Ответственным за разработку мер и контроль над обеспечением защиты информации в колледже является заведующий отделом информационной безопасности. Он осуществляет следующие виды работ по защите информации:

1. Контроль защищенности ИТ инфраструктуры Образовательного учреждения от угроз ИБ осуществляется посредством:

1) Проведения аудита безопасности ИС.

2) Контроля выполнения правил утвержденных политик безопасности администраторами и пользователями локальной сети учебного учреждения.

3) Контроля доступа к сетевым ресурсам.

2. Предотвращение, выявление, реагирование и расследование нарушений ИБ посредством:

1) Анализа и мониторинга журналов аудита критичных компонентов локальной сети учебного учреждения, включая активное сетевое оборудование, МЭ, серверы, рабочие станции и т.п.

2) Мониторинга сетевого трафика с целью выявления сетевых атак.

3) Контроля процесса создания новых учетных записей пользователей и предоставления доступа к ресурсам локальной сети учебного учреждения.

4) Опроса пользователей и администраторов информационных систем.

5) Внедрения и эксплуатации, специализированных программных и программно-технических средств защиты информации.

6) Координации деятельности всех структурных подразделений Образовательного учреждения по поддержанию режима ИБ.

Помимо этого, заведующим отделом информационной безопаснсоти осуществляется планирование и реализация организационных мер по обеспечению ИБ, включая:

1. Анализ и управление информационными рисками.

2. Разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов и других организационно-распорядительных документов по обеспечению ИБ.

3. Разработку планов мероприятий по повышению уровня ИБ Образовательного учреждения.

4. Обучение пользователей информационных систем, с целью повышения их осведомленности в вопросах ИБ.

Наряду с заведующим отделом информационной безопасности, в разработке и согласовании организационно-распорядительных и нормативных документов по защите информации, включая составление перечней информационных ресурсов, подлежащих защите, также участвуют следующие сотрудники колледжа:

1. Специалист по кадрам.
2. Юрисконсульт.
3. Функциональные подразделения, в которых обрабатывается информация, требующая защиты.

Наряду со специалистами ИСТП, пользователи ГБПОУ «ЮУГК», использующие информационные ресурсы, обязаны соблюдать все необходимые требования политик ИБ ГБПОУ «ЮУГК» и несут индивидуальную ответственность за нарушение требований данных политик.

Квалификационные требования, предъявляемые к сотрудникам подразделений, отвечающих за обеспечение ИБ, должны содержаться в должностных инструкциях сотрудников. Специалисты по защите информации должны проходить регулярную переподготовку и обучение.

Предоставление, изменение, отмена и контроль доступа к ресурсам локальной сети колледжа передачи данных производится сотрудниками ИСТП исключительно по утвержденным заявкам, в соответствии с «Политикой предоставления доступа пользователей в ЛСПД».

Сотрудники ИСТП отвечают за осуществление настройки параметров информационной безопасности серверов и рабочих станций локальной сети учебного учреждения передачи данных, в соответствии с утвержденными корпоративными стандартами, определяющими

требуемые уровни обеспечения защиты информации для различных структурных и функциональных компонентов локальной сети учебного учреждения. ИСТП отвечает за разработку соответствующих спецификаций и рекомендаций по настройке параметров безопасности, а также за осуществление контроля их исполнения.

Обеспечение внешних подключений локальной сети образовательной организации передачи данных Образовательного учреждения к сети Интернет и другим внешним сетям, предоставление сотрудникам удаленного доступа к локальной сети учебного учреждения и организация VPN-каналов связи осуществляется сотрудниками ИСТП с соблюдением требований информационной безопасности, определяемых «Политикой предоставления доступа к ресурсам сети Интернет» и «Политикой управления доступом к информационным ресурсам ЛСПД».

Договоры на обслуживание клиентов заключаются по утвержденной типовой форме функциональными подразделениями. Если договоры предполагают электронное обслуживание с использованием технологических ресурсов колледжа, то организация и контроль процедур безопасности осуществляется сотрудниками ИСТП.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к информации ограниченного доступа, либо к ИС образовательной организации, с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима ИБ при выполнении работ в ИС». Подготовка типовых вариантов этих соглашений осуществляется ИСТП образовательной организации, совместно с юридическим отделом.

ГЛАВА 3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА В КОЛЛЕДЖЕ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Особенности и ограничения на электронные образовательные ресурсы согласно требованиям информационной безопасности

Применение электронных образовательных ресурсов в образовательном процессе, актуальных в условиях реализации информационной безопасности с развитием технического прогресса, все существующие средства и методы неизбежно будут устаревать прежде, чем осуществится их внедрение в жизнедеятельность образовательных организаций. Это выдвигает на повестку дня осознание важности опережающего противодействия угрозам информационных атак на учебные заведения. Решить же проблему можно только в случае поддержки современных образовательных систем необходимыми финансовыми, нормативными, научно-методическими средствами и компетентными кадрами, способными обеспечить защиту этих систем от вредоносных технических, негативных интеллектуальных и разрушающих духовно-нравственных воздействий [57].

Нормативной составляющей в колледже на электронные образовательные ресурсы существуют правила работы персонала и обучающихся колледжа в компьютерных сетях и правила работы с ресурсами сети Интернет, входящие в Концепцию информационной безопасности колледжа, которые соответствуют требованиям обеспечения безопасности.

Правила работы с ресурсами сети Интернет, включая образовательные ресурсы

1.1. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Отдел информационного

обеспечения колледжа имеет право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

1.2. При работе с ресурсами сети Интернет недопустимо:

1.2.1. разглашение коммерческой и служебной информации колледжа, ставшей известной сотруднику колледжа по служебной необходимости либо иным путем;

1.2.2. распространение защищаемых авторскими правами материалов, затрагивающих какой- либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

1.2.3. публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

1.3. При работе с ресурсами Интернет запрещается:

1.3.1. загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

1.3.2. использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой колледжа.

1.4. Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политикой колледжа.

1.5. Вся информация о ресурсах, посещаемых сотрудниками и студентами колледжа, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а также администрации колледжа для детального изучения.

Правила работы персонала и обучающихся колледжа в компьютерных сетях

1. Данные правила регулируют права и обязанности обучающихся, связанные с работой в компьютерной сети колледжа и сети Интернет (далее Сетей), а также основные правила работы и полномочия преподавателей и сотрудников колледжа. Правила призваны обеспечить и организовать использование образовательного потенциала Сетей в сочетании с системой мер по обеспечению охраны и безопасности студентов.

2. Основными принципами политики колледжа для работы в Сетях являются:

- равный доступ для всех обучающихся;

- использование Сетей обучающимися только для образовательных целей.

- защита обучающихся от вредной или незаконной информации, содержащей: порнографию, пропаганду насилия и терроризма,

этнической и религиозной нетерпимости, наркотиков, азартных игр и т.п.

3. Полномочия преподавателей и сотрудников.

3.1. Начальник отдела по безопасности:

- организует и руководит всей деятельностью по реализации настоящих Правил;

- обеспечивает свободный и равный доступ обучающихся к Сетям в соответствии с учебной программой и возможностями колледжа;

- организует и руководит всей деятельностью по реализации настоящих Правил;

- обеспечивает свободный и равный доступ обучающихся к Сетям в соответствии с учебной программой и возможностями колледжа;

- отвечает за организацию мер, включая сотрудничество с провайдером, по ограничению доступа обучающихся к ресурсам вредного или незаконного содержания в Сетях в соответствии с действующим законодательством;

- обеспечивает контроль за соблюдением правил работы, обучающихся в сетях;

- организует поддержку и обновление сайта. Размещает на сайте только материалы, утвержденные директором;

- незамедлительно сообщает директору о выявлении нарушений и принимает меры по устранению нарушений.

3.2. Преподаватели компьютерных классов обязаны:

- объяснять обучающимся правила безопасного и ответственного поведения при работе в Сетях;

- использовать возможности Интернет в целях обогащения и расширения образовательной деятельности, для чего обучающимся назначать конкретные задания;

- осуществлять непрерывный контроль работы обучающихся в Сетях в учебное время;

- принимать незамедлительные меры для прекращения доступа обучающихся к ресурсам запрещенного содержания в Сетях;

- немедленно сообщать начальнику отдела по безопасности или директору о нарушении правил или о создании незаконного контента в сети колледжа;

- не покидать учебный кабинет во время пары, и не допускать обучающихся во время перемены к работе в Сетях.

3.3. Преподаватели несут ответственность за целостность оборудования колледжа, закрепленного за учебным кабинетом, в котором проводят занятия.

3.4. Сетевой администратор обязан:

- обеспечивать общую безопасность и эффективность работы в Сетях;

- предлагать и осуществлять меры по ограничению доступа обучающихся к вредным или незаконного содержания ресурсам в Сетях в соответствии с законодательством;

- периодически просматривать содержимое Сети колледжа с целью предотвращения любых возможных угроз и рисков безопасности для обучающихся;

- немедленно сообщать начальнику отдела по безопасности или директору о нарушении Правил или о создании незаконного контента в сети колледжа.

4. Права и обязанности обучающихся

4.1. Обучающиеся имеют право:

- на равный доступ к Сетям с учетом политики информатизации колледжа;

- на получение доступа к сети Интернет (только под наблюдением преподавателя);

- на грамотное и ответственное обучение работе в Сетях;

- быть информированным о правилах работы в Сетях.

4.2. Обучающиеся обязаны соблюдать следующие правила:

- использовать Сети только для образовательных целей;

- запрещается выход на сайты, не включенные в перечень преподавателем для данного занятия;

- немедленно сообщить преподавателю при обнаружении материалов, содержащих порнографию, пропаганду насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр, и т.п.;

- запрещается проводить любую деятельность, которая угрожает целостности компьютерной сети колледжа или атаки на другие системы;

- запрещено использование нелицензионного программного обеспечения, защищенных авторским правом материалов без разрешения, и любой другой деятельности, которая нарушает авторские права.

5. Ответственность

5.1. Обучающиеся за нарушение положений настоящих Правил привлекаются к дисциплинарной ответственности в соответствии с правилами внутреннего распорядка колледжа.

5.2. Преподаватели и сотрудники за нарушение положений настоящих Правил несут ответственность в соответствии с Трудовым кодексом и привлекаются к дисциплинарной ответственности.

5.3. За нарушения, которые являются преступлениями, административными нарушениями или причиняют ущерб собственности, виновные несут ответственность в соответствии с законодательством РФ.

Таким образом, для обеспечения информационной безопасности электронных образовательных ресурсов в образовательных организациях, необходимо соблюдать следующие меры:

1. Обеспечение целостности и достоверности образовательной информации, важной для поступательного развития личности обучающихся и преподавателей;

2. Обеспечение конфиденциальности образовательной информации – ее защищенности от несанкционированного доступа к ней посторонних лиц;

3. Обеспечение доступности образовательной информации – возможности за приемлемое время получить требуемую информационную услугу;

4. Обеспечение оптимального состояния вспомогательной инфраструктуры, поддерживающей работу и сохранность электронной системы образования.

3.2. Рекомендаций по защите электронного образовательного ресурса по профессиональному модулю «Обработка отраслевой информации» в ГБПОУ «Южно-Уральский государственный колледж»

Все программное обеспечение веб-приложений очень сложное, и каждое приложение имеет проблемы с безопасностью, которые время от времени обнаруживаются, как правило, с использованием некоторой комбинации входных данных, которые программисты не ожидали.

С учетом проведенного анализа защищенности электронных образовательных ресурсов, выявленных тенденций обеспечения информационной безопасности информационных ресурсов колледжа реализовали электронный образовательный ресурс, используя SQL-инъекции и защиты текста на страницах разделов (использование скрипта для запрета копирования**,** запрет выделения текста в CSS-стилях).

SQL-инъекции. SQL-инъекция представляет собой выполнение произвольного запроса к базе данных приложения с помощью поля формы или параметра URL. В случае использования стандартного языка Transact SQL возможно вставить вредоносный код. В результате чего

будут получены, изменены или удалены данные таблиц. Чтобы предотвратить это, используйте параметризованные запросы, которые поддерживаются большинством языков веб-программирования.

Рассмотрим запрос:

```
SELECT * FROM table WHERE column = 'parameter';
```

Если злоумышленник изменит значение parameter на ' OR '1'='1, запрос примет следующий вид:

```
SELECT * FROM table WHERE column = '' OR '1'='1';
```

Так как '1' равен '1', атакующий получит доступ ко всем данным таблицы. Это позволит выполнить произвольный запрос, добавив в конец выражения SQL.

Уязвимость этого запроса легко устранить с помощью параметризации. Например, для приложения, написанного с использованием PHP и MySQLi, он выглядит так:

```
1 $stmt = $pdo->prepare('SELECT * FROM table WHERE column = :value');
2 $stmt->execute(array('value' => $parameter));
```

Межсайтовый скриптинг (XSS) — тип атаки на веб-ресурсы, заключающийся во внедрении в страницу сайта вредоносного кода, который выполняется на компьютере пользователя, изменяет страницу и передаёт украденную информацию злоумышленнику.

Например, если на странице комментариев нет проверки входных данных, злоумышленник внедряет вредоносный код JavaScript. В результате у пользователей, которые просматривают комментарий, выполняется код, и данные об авторизации из cookies-файлов отправляются атакующему.

Особенно подвержены этому виду атаки современные веб-приложения, где страницы построены из пользовательского контента, интерпретируемого фронтенд-фреймворками вроде Angular и Ember. В эти фреймворки встроена защита от межсайтового скриптинга, но

смешанное формирование контента на стороне сервера и клиента создает новые комплексные атаки: внедрение директив Angular или хелперов Ember.

При проверке сосредоточьтесь на пользовательском контенте, чтобы избежать некорректной интерпретации браузером. Это похоже на защиту от SQL-инъекций. При динамической генерации HTML-кода используйте специальные функции для изменения и получения значений атрибутов (например, element.setAttribute и element.textContent), а также шаблонизаторы, которые выполняют экранизацию специальных символов автоматически.

Политика безопасности содержимого (CSP) — ещё один инструмент защиты от XSS-атак. CSP — заголовки сервера, определяющие белый список источников, откуда разрешена загрузка данных для разных типов ресурсов. Например, запрет запуска скриптов со стороннего домена или отключение функции eval(). Благодаря политикам CSP даже при внедрении вредоносного кода в страницу его выполнение становится невозможным.

Следующая мера информационной защиты многопользовательского электронного практикума - защита текста на главной странице или на страницах разделов.

Контент на этих страницах копируют, в основном, вручную. Поэтому, здесь применимы следующие методы.

1. *Использование скрипта для запрета копирования***.** На странице можно добавить скрипт, который не позволит пользователю вручную выделить и скопировать текст.

Пример скрипта приведен на рисунке 21.

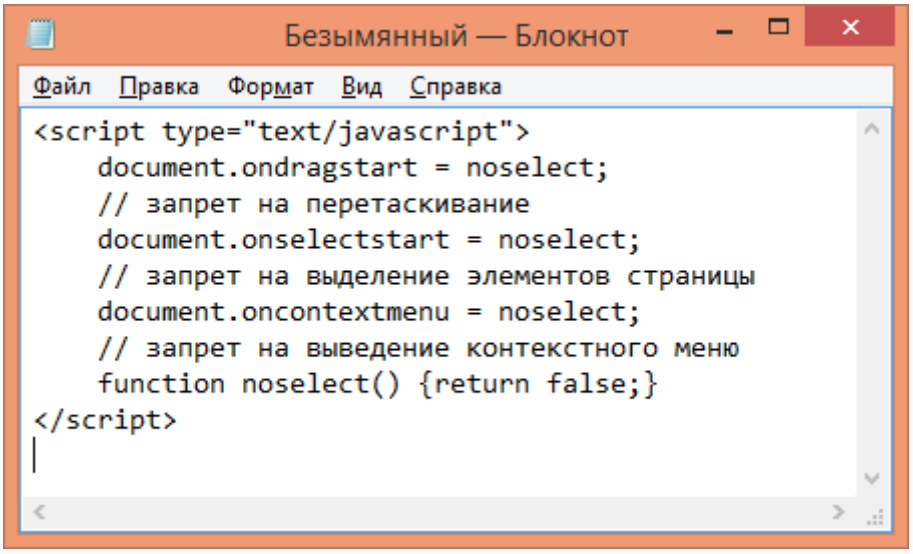


Рисунок 21 – Пример скрипта

Приведенный выше скрипт запрещает выделение части текста, а также отключает контекстное меню во всем документе, если злоумышленник захочет открыть код страницы.

Минус данного способа в том, что пользователи иногда переходят по ссылкам, кликая правой клавишей мыши. Подобными скриптами можно создать ряд неудобств и понизить количество просмотров страниц своего сайта, и соответственно, конверсию в целевые действия.

Этот метод легко обойти, открыв источник страницы через главное меню браузера, либо отключив в браузере скрипты и копируя необходимое без всяких запретов. Однако, вероятность воровства текста неопытным «копирайтером» существенно снизится.

2. *Запрет выделения текста в CSS-стилях.* Аналогичный предыдущему методу, но можно уже не использовать скрипт, а прописать отдельный стиль (например, класс «noselect»), в котором запрещается выделять текст.

Пример кода приведен на рисунке 22.

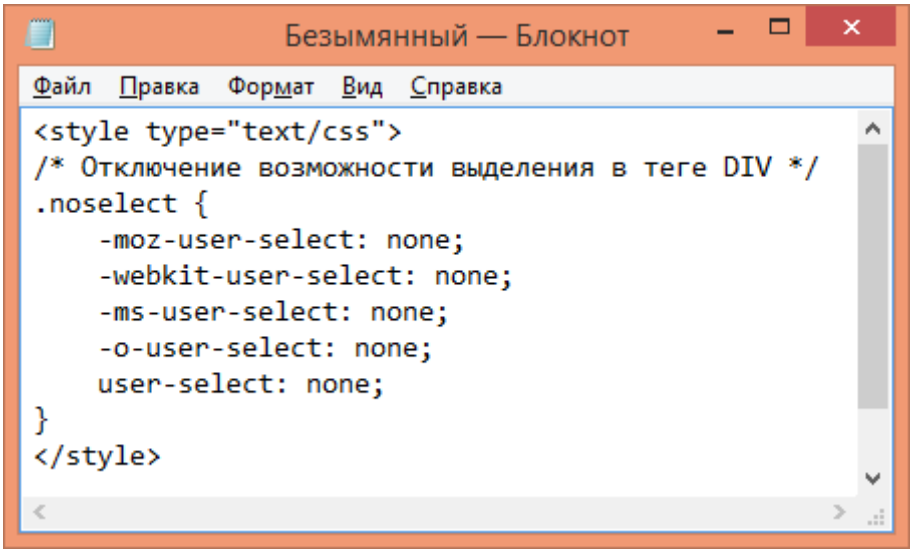


Рисунок 22 – Пример кода

Этот метод имеет уже немного меньше недостатков: с помощью отключения скриптов возможности выделения текста все равно не будет, а отключить стили в браузере сложнее, однако, этот метод все также легко обойти, если открыть HTML-код страницы.

Распределяйте права доступа к файлам

Разрешения файла (file permissions) определяют КТО и ЧТО может с ним делать.

В *nix системах у файлов 3 варианта доступа, которые представляются в виде цифр:

- «Read» (4) — чтение содержимого файла;
- «Write» (2) — изменение содержимого файла;
- «Execute» (1) — выполнение программы или скрипта.

Чтобы установить множественные разрешения, достаточно сложить их числовые значения:

- «Чтение» (4) + «запись» (2) = 6;
- «Чтение» (4) + «запись» (2) + «выполнение» (1) = 7.

При распределении прав пользователи делятся на 3 типа:

1) «Owner» (владелец) — создатель файла (изменяем, но может быть только один);

2) «Group» (группа) — группа пользователей, которые получают разрешения;

3) «Others» (прочие) — остальные пользователи.

Установка владельцу прав доступа на чтение и запись, группе — на чтение, прочим — запрет доступа выглядит так:

	Чтение	Запись	Выполнение
Владелец	2	4	0
Группа	0	4	0
Прочие	0	0	0

Итоговое представление: 640.

Для каталогов аналогично, но флаг «выполнить» значит сделать рабочей директорией. При установке CMS-разрешения, как правило, устанавливаются корректно с точки зрения безопасности. Однако в Интернете часто советуют решать проблемы прав доступа установкой на все файлы значения 666 или 777. Этот совет помогает решить проблему, но открывает серьёзную уязвимость, потому что всем появляется право изменить (вставить вредоносный код) или удалить файлы на сервере.

Распределяйте права доступа к файлам на сервере в соответствии с задачами пользователей.

3.3. Экспериментальная проверка электронного образовательного ресурса по профессиональному модулю «Обработка отраслевой информации» в ГБПОУ «Южно-Уральский государственный колледж»

Внедрение вышеописанных мер привело к повышению уровня информационной безопасности при использовании ЭОР в ГБПОУ «Южно-Уральский государственный колледж».

Основным показателем обеспечения безопасности электронного образовательного ресурса является повторный анализ количества обращений к исполняемому файлу запуска программы и файлу сбора и

обобщения результатов тестирования при проведении контроля знаний обучающихся.

Разработанные и внедренные нами методы, а именно: разработка рекомендаций для педагогического состава образовательной организации направленные на формирование компактности в области информационной безопасности, ограничение доступа к программным и исполняемым файлам электронного образовательного ресурса, установка программы удаленного доступа для контроля деятельности студентов колледжа во время работы с электронным образовательным ресурсом, позволили сократить данный показатель к абсолютному минимуму, так как у обучающихся заблокирован доступ не только к исходному файлу, а так же к файловой системе компьютера в целом.

Доступ к исполняемому файлу запуска электронного образовательного ресурса остался открытым для студентов, но при этом из общего доступа были убраны исходные файлы проекта. Повторный анализ выявил 12 обращений к исполняемому файлу запуска ЭОР, подробная информация изменений представлена на рисунке 23.

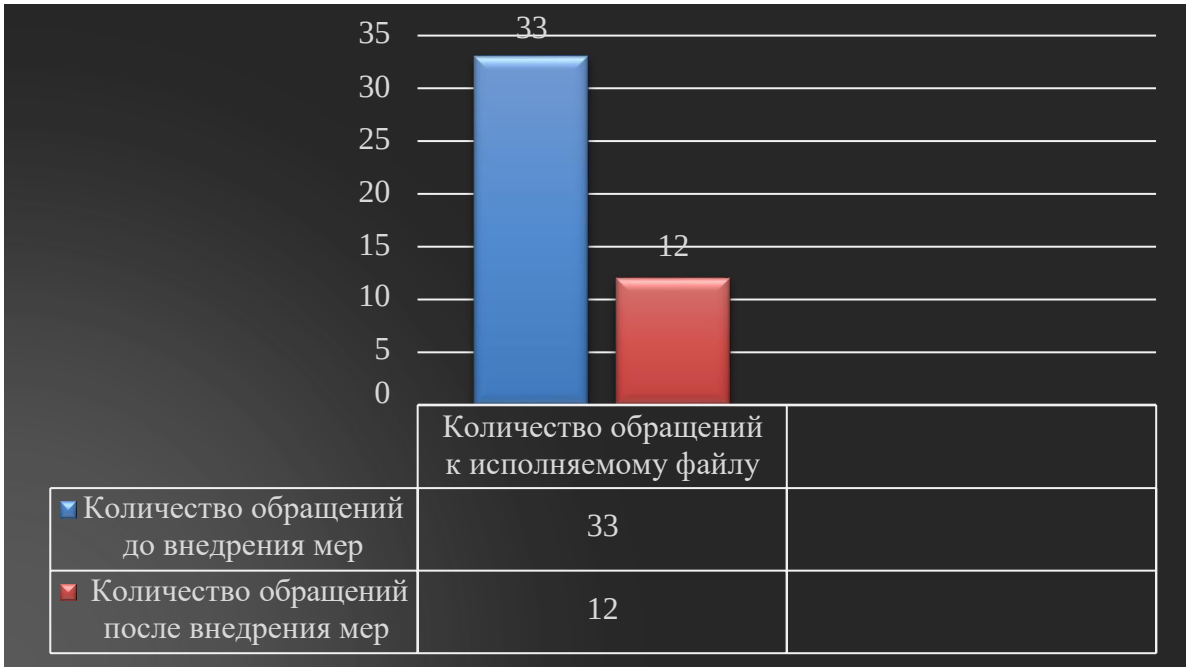


Рисунок 23 - Динамика изменений количества запросов к файлам

Положительно сказались рекомендации для преподавателей в вопросе обеспечения информационной безопасности, преподаватели сменили пароли на более сложные, а также активировали функцию учетной записи обязывающую пользователя менять пароль каждые 30 дней.

Внедрение программы удалённого доступа позволило преподавателям более эффективно осуществлять контроль за деятельностью обучающихся как во время тестирования, так и во время выполнения заданий.

Результаты бета-тестирования разработанного нами электронного образовательного ресурса по профессиональному модулю «Обработка отраслевой информации» оцениваем положительно и считаем доказанной гипотезу исследования.

Таким образом, можно выделить следующие меры информационной защиты электронного образовательного ресурса по профессиональному модулю «Обработка отраслевой информации» в ГБПОУ «ЮУГК»:

1. Настройка политики безопасности сайта.
2. Распределение прав доступа к файлам.
3. SQL-инъекции.
4. Защита текста на главной странице или на страницах разделов (использование скрипта для запрета копирования, запрет выделения текста в CSS-стилях).

Выводы по Главе III

В рамках третьей главы нашего исследования были разработаны рекомендации по защите электронного образовательного ресурса в ГБПОУ «ЮУГК» и представлено их обоснование.

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Информационный бюллетень «Архитектура и стратегия информационной безопасности Cisco».
[2] Стратегии развития холдинга «РЖД» на период до 2030 года, утвержденная советом директоров ОАО «РЖД» от 23 декабря 2013 г. № 19.
[3] Стратегия научно-технологического развития холдинга «РЖД» на период до 2025 года и на перспективу до 2030 года (Белая книга).
[4] Концепция по обеспечению кибербезопасности ОАО «РЖД.
[5] Концепция обеспечения информационной безопасности ЗАО «Страховая компания «Диана».
[6] Концепция информационной безопасности информационных систем персональных данных администрации Шемуршинского района.
[7] Концепция информационной безопасности информационных систем персональных данных ГАОУ СПО «Республиканский базовый медицинский колледж имени Э.Р. Раднаева».
[8] Концепция информационной безопасности информационных систем Министерства социальной, семейной и демографической политики Удмуртской Республики.
[9] Концепция информационной безопасности информационных систем персональных данных ООО «АТЭКС ПЛЮС».
[10] Политика информационной безопасности ФГБУ «ПИЯФ» НИЦ «Курчатовский институт».
[11] Политика информационной безопасности ГПОАУ ЯО «Ярославского педагогического колледжа».
[12] СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
[13] РС БР ИББС-2.0-2007 «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0».
[14] СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014».
[15] Политика информационной безопасности комитета Ставропольского края по делам архивов.
[16] Политика информационной безопасности при работе с персональными данными в администрации Нефтекумского городского округа Ставропольского края.
[17] Политика информационной безопасности в ГАУЗ «СП №8».
[18] Политика информационной безопасности информационных систем персональных данных ГУЗ «Поликлиника №5».
[19] Политика Torex в области информационной безопасности.
[20] Политика информационной безопасности ООО «Юсодент».
[21] Соглашение о порядке защиты конфиденциальной информации и ответственности за ее разглашение при осуществлении Евразийской экономической комиссией полномочий по контролю за соблюдением единых

правил конкуренции.
[22] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
[23] Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
[24] «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ.
[25] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
[26] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
[27] Политика «Обработка персональных данных в ПАО «МТС» ПТ-010-3.
[28] ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
[29] «План мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации»
(утв. Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18.12.2017 № 2).