Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

ДЕМОНСТРАЦИОННЫЙ МАТЕРИАЛ С ЭЛЕМЕНТАМИ ИНТЕРАКТИВНОСТИ «СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ»

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Информационная безопасность»

Идентификационный номер ВКР: 142

Екатеринбург 2018

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующая кафедрой ИС
_____ Н. С. Толстова
«____» _____ 2018 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ДЕМОНСТРАЦИОННЫЙ МАТЕРИАЛ С ЭЛЕМЕНТАМИ ИНТЕРАКТИВНОСТИ «СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ»

Исполнитель: Климчик А.М.
обучающийся группы № ИБ-401
Руководитель: Окуловская А.Г.
старший преподаватель
Нормоконтролер: Рыжкова Т.В.

Екатеринбург 2018

АННОТАЦИЯ

Выпускная квалификационная работа состоит из демонстрационного материала с элементами интерактивности по социальной инженерии и пояснительной записки на 50 страницах, содержащей 35 рисунков, 32 источника литературы, а также 1 приложение на 2 страницах.

Ключевые слова: ИНТЕРАКТИВ, ДЕМОНСТРАЦИЯ, ИНЖЕНЕРИЯ, СОЦИАЛЬНАЯ.

Климчик А.М., Демонстрационный материал с элементами интерактивности «Социальная инженерия»**:** выпускная квалификационная работа / А.М. Климчик; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2017. — 50 с.

Данная выпускная квалификационная работа содержит в себе демонстрационный материал с элементами интерактивности по социальной инженерии с применением интерактивных технологий. Цель работы: разработать демонстрационный материал с элементами интерактивности «Социальная инженерия».

При разработке электронного пособия были использованы такие технологии как язык гипертекстовой разметки HTML, CSS, визуальный HTML-редактор Notepad, для создания презентаций был использован MS PowerPoint, интерактивные приложения были разработаны в ресурсе learningapps.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Важной частью информационной безопасности является человеческий фактор, ведь как однажды написал в своей книге «Секреты и ложь. Безопасность данных в цифровом мире» Брюс Шнайер: «обеспечить компьютерную безопасность трудно (может быть, даже невозможно), однако представьте на минуту, что нам это удалось сделать. Где необходимо, применяется мощная криптография, протоколы безопасности безупречно выполняют свои функции. В нашем распоряжении имеются как надежное оборудование, так и надежное программное обеспечение. Даже сеть, в которой мы работаем, совершенно безопасна. Чудесно! К несчастью, этого еще недостаточно. Сделать что-либо полезное эта замечательная система может лишь при участии пользователей. И это взаимодействие человека с компьютером таит в себе наибольшую угрозу из всех существующих. Люди часто оказываются самым слабым звеном в системе мер безопасности, и именно они постоянно являются причиной неэффективности последних. В отношении безопасности математический аппарат безупречен, компьютеры же уязвимы, сети вообще паршивы, а люди просто отвратительны» [4, с.56].

Именно поэтому в качестве темы выпускной квалификационной работы была выбрана социальная инженерия (СИ). Социальная инженерия – это метод получения доступа к определенной информации, который основывается на особенности психологии людей. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, такой как пароли, банковские данные и так далее.

Каждый в жизни, наверное, сталкивался с тем, что кто-то на него воздействовал методами социальной инженерии, но, скорее всего, оба этих человека (и жертва, и охотник) не догадывались об этом. Вы можете столкнуться с этим в магазине, когда вам пытаются продать какой-либо товар. Или по телевидению, когда вам рекламируют «замечательный» товар, который на

самом деле далеко не «замечательный», и так далее. Но, как вы заметили, во всех этих ситуациях никто не догадывается о том, как именно происходит воздействие на сознание, как именно вас побуждают совершить то или иное действие (ежесекундно проанализировать ситуацию под силу лишь опытным рекламщикам и маркетологам) просто потому, что обычно этому не учат.

Многие компании тратят сотни тысяч долларов на организацию корпоративной компьютерной безопасности. Эта безопасность позволяет защищать секреты компании, помогает соблюдать федеральные законы и обеспечивает конфиденциальность клиентов компании. К сожалению, даже лучшие механизмы безопасности могут быть обойдены с помощью социальной инженерии. Социальная инженерия использует очень дешевые и нетехнологические средства для того, чтобы преодолеть препятствия, создаваемые механизмами информационной безопасности.

Конечные цели обмана так же весьма разнообразны. Одной из актуальных целей в концепции характера развития отношений между производителями на сегодняшний день является получение несанкционированного доступа к конфиденциальной информации.

К счастью, подавляющее большинство мошенников действует по идентичным или близким шаблонам. Поэтому изучение приемов их «работы» позволяет распознать обман и не попасться на удочку, а также выработать способы и методы противодействия им.

В связи с выше сказанным было принято решение разработать демонстрационный материал с элементами интерактивности «Социальная инженерия». Для удобства использования подобного демонстрационного материала решено собрать все материалы на HTML. В данный материал будет включена теория по социальной инженерии и способ защиты от подобного вида атак.

Данный демонстрационный материал будет использоваться в рамках дисциплины «Информационная безопасность и защита информации».

Объект работы – процесс формирования знаний в области социальной инженерии.

Предмет работы – учебные материалы по теме «Социальная инженерия».

Цель работы – разработать демонстрационный материал с элементами интерактивности «Социальная инженерия».

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ источников по теме «Социальная инженерия».
2. Проанализировать рабочую программу по дисциплине «Информационная безопасность и защита информации».
3. Изучить источники по формированию интерфейса для демонстрационного материала.
4. Разработать демонстрационный материал с элементами интерактивности «Социальная инженерия».

В соответствии с указанными целями и задачами данная работа будет иметь следующую структуру: введение, две главы, заключение и приложение.

В первой главе рассматриваются различные источники как печатные, так и электронные по теме, также анализируется литература по интерактивному обучению и созданию сайтов с помощью HTML.

Во второй главе выпускной квалификационной работы описывается непосредственно разрабатываемый демонстрационный материал.

В заключении приводятся выводы о решении поставленных задач исследования и о проделанной работе.

1 АНАЛИЗ ПЕЧАТНЫХ И ИНТЕРНЕТ-ИСТОЧНИКОВ

1.1 Анализ печатных источников

Прежде чем начать разрабатывать демонстрационный материал «Социальная инженерия» были проанализированы различные печатные и интернет-источники. Так как СИ заключается в прямом контакте между людьми, очень много источников имеют направление в сторону психологии и изучении межличностных отношений.

Рисунок 1 — Обложка книги «Искусство обмана»

Книга «Искусство обмана» [10] (рисунок 1) доказывает, насколько мы все уязвимы. В современном мире, где безопасность подчас выходит на первый план, на защиту компьютерных сетей и информации тратятся огромные деньги. Деньги тратятся на технологии безопасности. Эта книга объясняет, как просто бывает перехитрить всех защитников и обойти технологическую оборону, как работают социальные инженеры и как отразить нападение с их стороны. Кевин Митник и его соавтор, Бил Саймон рассказывают множество историй, которые раскрывают секреты социальной инженерии. Авторы дают практические советы по защите от атак, по обеспечению корпоративной безопасности и снижению информационной угрозы. «Искусство обмана» не

только демонстрирует, насколько опасна и вредоносна социальная инженерия, но и поможет разработать собственную программу тренинга по безопасности для сотрудников компании.

Истории, рассказанные во второй книге Кевина Мтиника «Искусство вторжения» [9] (рисунок 2), демонстрируют, как небезопасны все компьютерные системы, и как мы уязвимы перед подобными атаками. Урок этих историй заключается в том, что хакеры находят новые и новые уязвимости каждый день. Читая эту книгу, думайте не о том, как изучить конкретные уязвимости тех или иных устройств, а о том, как изменить ваш подход к проблеме безопасности и приобрести новый опыт. Если вы профессионал в области информационных технологий или обеспечения безопасности, каждая из историй станет для вас своеобразным уроком того, как повысить уровень безопасности в вашей компании. Если же вы не имеете отношения к технике и просто любите детективы, истории о рисковых и мужественных парнях – вы найдете их на страницах этой книги.

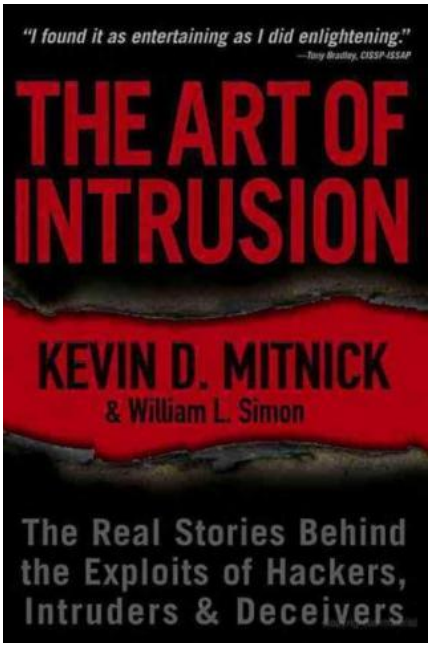

Рисунок 2 — Обложка книги «Искусство вторжения»

Хенрик Фексеус, знаменитый шведский психолог и специалист по невербальной коммуникации, в своей книге «Искусство манипуляции. Как читать мысли других людей и незаметно управлять ими» [27] (рисунок 3) даёт

хорошее и понятное описание различным техникам и методикам нейролингвистического программирования (НЛП). Раскрывает, как правильно ими пользоваться. Даёт конкретные указания, как работать со своими жестами, своими эмоциями и мыслями, и как на основе всего этого управлять мыслями другого человека.

Рисунок 3 — Обложка книги «Искусство манипуляции. Как читать мысли других людей и незаметно управлять ими»

В книге Кузнецова и Симдянова «Социальная инженерия и социальные хакеры» [13] (рисунок 4) описан арсенал основных средств современного социального хакера (трансактный анализ, нейролингвистическое программирование), рассмотрены и подробно разобраны многочисленные примеры социального программирования (науки, изучающей программирование поведения человека) и способы защиты от социального хакерства. Книга написана довольно простым языком, именно поэтому будет понятна, как и IT-специалистам, сотрудникам служб безопасности предприятий, психологам, изучающим социальную инженерию и социальное программирование, так и обычным пользователям ПК, поскольку именно они часто выбираются социальными хакерами в качестве наиболее удобных мишеней.

Рисунок 4 — Обложка книги «Социальная инженерия и социальные хакеры»

В своей третье книге «Призрак в сети» [11] (рисунок 5) Кевин Митник описал свою жизнь и свою деятельность в роли хакера, ведь в своё время про него говорили примерно так: «Он по праву считается самым неуловимым мастером компьютерного взлома в истории. Он проникал в сети и компьютеры крупнейших мировых компаний, и как бы оперативно ни спохватывались власти, Митник был быстрее, вихрем проносясь через телефонные коммутаторы, компьютерные системы и сотовые сети. Он долгие годы рыскал по киберпространству, всегда опережая преследователей не на шаг, а на три шага, и заслужил славу человека, которого невозможно остановить» [11, с.23] Но для Митника хакерство не сводилось только к технологическим эпизодам, он плел хитроумные сети обмана, проявляя редкое коварство и выпытывая у ничего не подозревающего собеседника ценную информацию. «Призрак в Сети» – захватывающая невыдуманная история интриг, саспенса и невероятных побегов. Это портрет провидца, обладающего такой изобретательностью, хваткой и настойчивостью, что властям пришлось полностью переосмыслить стратегию погони за ним. Отголоски этой эпической схватки чувствуются в сфере компьютерной безопасности и сегодня.

Рисунок 5 — Обложка книги «Призрак в сети»

В книге Пола Экмана «Психология лжи. Обмани меня, если сможешь» [17] автор даёт исчерпывающие ответы на такие вопросы, как: правда ли, что современный человек в среднем лжет трижды за десять минут разговора? Как реагировать на то, что ложь проникла во все сферы человеческой жизни? Что делать, если не удается распознать ложь по словам и голосу? Рассказывает про универсальные микровыражения и микрожесты, которые всегда могут выдать лжеца, независимо от социального статуса и национальной принадлежности. Данная книга учит замечать то, чего не видят другие. Книга адресована всем, кто заинтересован в разоблачении лжи: политикам и бизнесменам, врачам и юристам, психологам, педагогам, менеджерам, домохозяйкам, всем, кто не хочет становиться жертвой обмана и психологических манипуляций в профессиональной и личной жизни.

В своей книге «Психология влияния. Как научиться убеждать и добиваться успеха» [21] (рисунок 6) Роберт Чалдини, доктор наук, профессор психологии и признанный эксперт в сфере влияния и убеждения, рассматривает шесть универсальных приемов, благодаря которым вы станете настоящим мастером уговоров. В то же время, зная об этих приемах, вы всегда

сможете избежать нежелательного воздействия со стороны. Так же автор поднимает отношение людей к искусству убеждения. «Одни стремятся овладеть им в совершенстве, чтобы всегда и везде добиваться своих целей, другие считают недопустимым, когда, используя механизмы воздействия, людям навязывают невыгодные для них условия. Однако никто из нас не хочет стать жертвой манипуляторов, легкой добычей для продавцов, сборщиков средств и рекламодателей».

Рисунок 6 — Обложка книги «Психология влияния. Как научиться убеждать и добиваться успеха»

Книга Эрика Берна «Игры, в которые играют люди. Психология человеческих взаимоотношений» [30] (рисунок 7) считается одной из основополагающих культовых книг по психологии человеческих взаимоотношений. Система, разработанная Берном, призвана избавить человека от влияния жизненных сценариев, программирующих его поведение, научить его меньше "играть" в отношениях с собой и другими, обрести подлинную свободу и побудить к личностному росту. В этой книге автор даёт много полезных советов, которые помогут понять природу человеческого общения, мотивы собственных и чужих поступков и причины возникновения конфликтов. По

мнению автора, судьба каждого из нас во многом определяется еще в раннем детстве, однако в зрелом возрасте она вполне может быть осознана и управляема человеком, если он этого захочет.

Рисунок 7 — Обложка книги «Игры, в которые играют люди»

Книга Альфреда Адлера «Понять природу человека» [1] является попыткой познакомить широкую публику с основами психологии личности. В то же время в ней демонстрируется практическое применение психологических принципов не только для выстраивания наших повседневных отношений с окружающим миром и другими людьми, но и для организации нашей внутренней жизни. В основу этой книги положен годичный цикл лекций, прочитанных перед аудиторией, состоящей из сотен мужчин и женщин всех возрастов и профессий, в народном институте Вены. Цель этой книги — во-первых, показать, как неверно выбранная линия поведения одного человека вносит дисгармонию в нашу общественную жизнь; во-вторых, научить отдельных людей распознавать и признавать свои ошибки и, наконец, показать им, как гармонично адаптироваться к социальной среде.

1.2 Анализ интернет-источников

В статье «Социальная инженерия для начинающих» [23] (рисунок 8) раскрывается понятие социальной инженерии (СИ) и чем она занимается. Также в ней описываются виды и методы СИ, такие, как:

- спешка, создание дефицита времени, чтобы лишить оппонента времени на размышление и проверку данных;
- провоцирование и ирония;
- подозрительность и безразличие (чтобы у оппонента появилось желание оправдываться).

Также автор рассматривает СИ со стороны мошенничества и заработка денег и даёт хорошие книги Кевина Митника по данной теме.

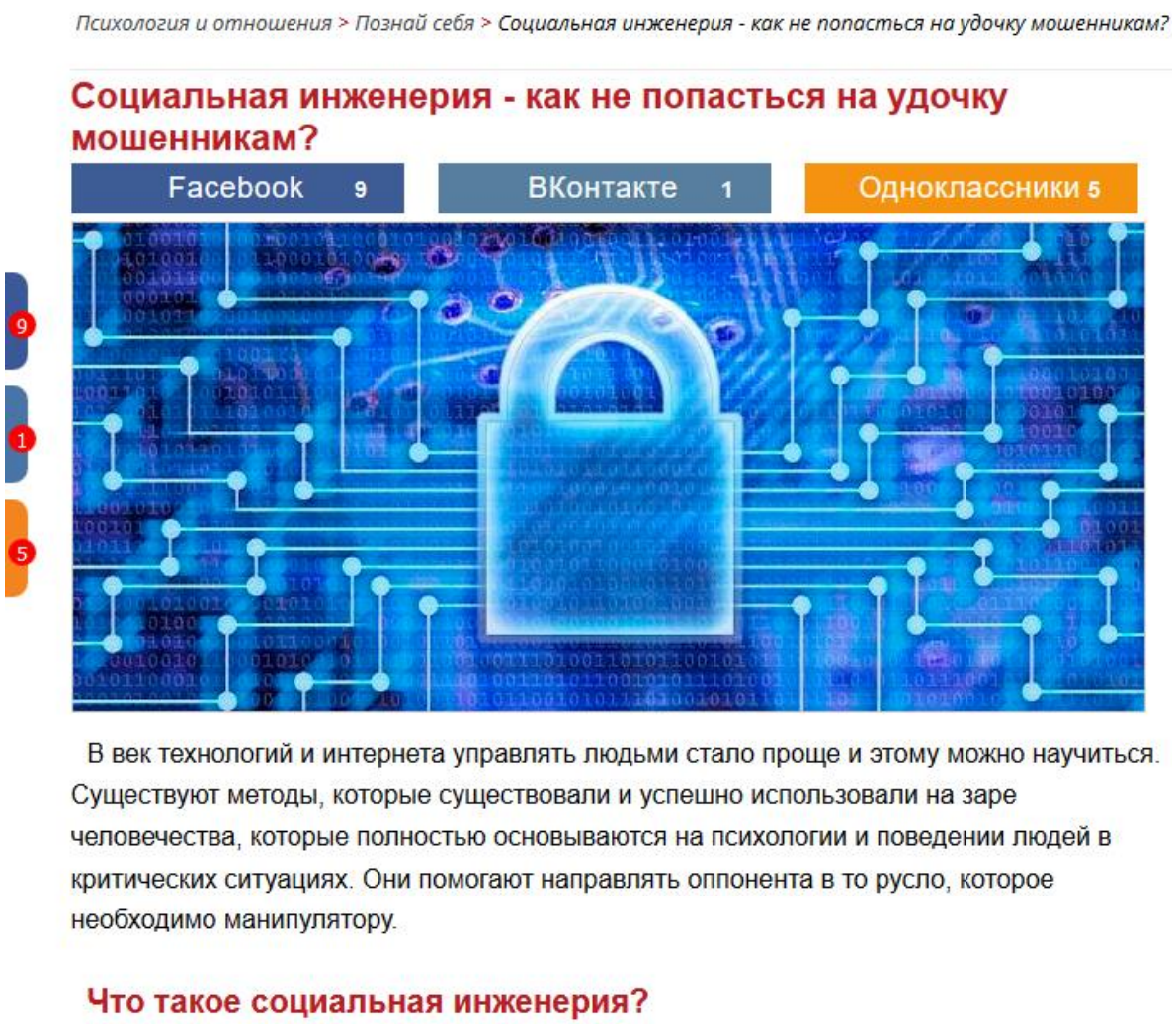

Рисунок 8 — Статья «Социальная инженерия для начинающих»

Изначально в понятии «Социальная инженерия» отсутствовал четкий оттенок злонамеренности. Оно применялось для обозначения комплекса специфических знаний, которые позволяют управлять процессом создания, модернизации и воспроизведения некой искусственно созданной реальности, используемой в изобретательской деятельности. Именно эту мысль раскрывают в статье «Определение понятия социальной инженерии и её наполнения» [14] (рисунок 9) и дают различные определения социальной инженерии.

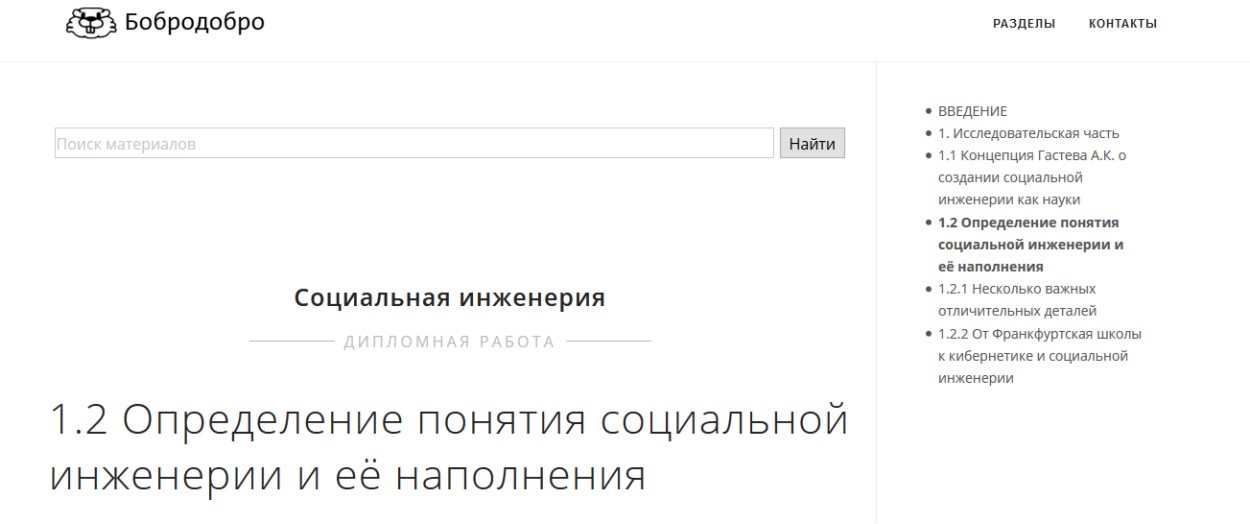

Рисунок 9 — Статья «Определение понятия социальной инженерии и её наполнения»

«Лаборатория Касперского» — международная компания, специализирующаяся на разработке систем защиты от компьютерных вирусов, спама, хакерских атак и прочих кибер угроз. Компания ведёт свою деятельность более чем в 200 странах и территориях мира. Центральный офис «Лаборатории Касперского» находится в Москве. Компания входит в четвёрку ведущих мировых производителей программных решений для защиты конечных устройств (Endpoint Protection). Но лаборатория Касперского не может учитывать человеческий фактор при защите компьютеров, именно поэтому они выпустили статью [26] (рисунок 10) в которой раскрывают, что из себя представляет СИ и как можно себя обезопасить от этого.

Рисунок 10 — Статья «Социальная инженерия, или, как взломать человека»

В статье «СИ. Что такое социальная инженерия и методы защиты» [22] (рисунок 11) описываются различные методики социальной инженерии с примерами. Цель данной статьи описать это всё обычному пользователю, который не особо посвящён в тонкости информационной безопасности и психологии.

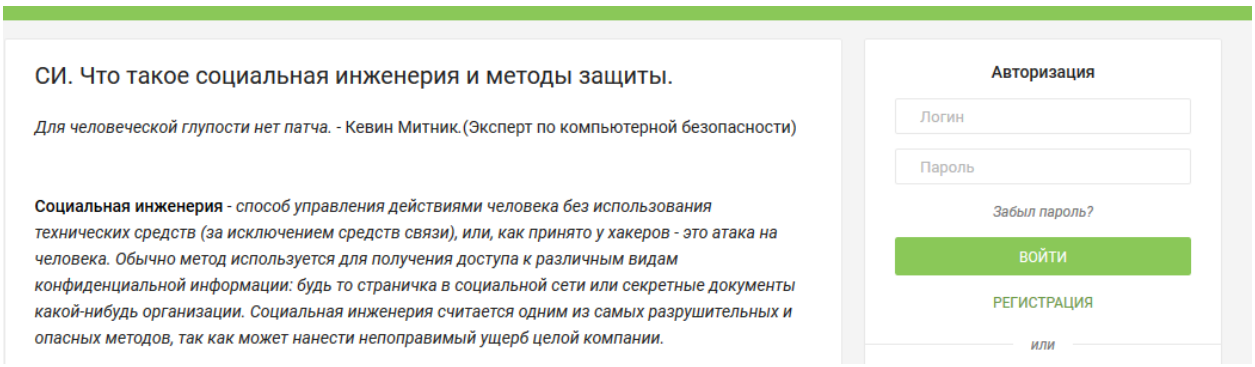

Рисунок 11 — Статья «СИ. Что такое социальная инженерия и методы защиты»

В статье «Понятия социальная инженерия» [19] термин «Социальная инженерия» рассматривается намного шире и обозначает любые способы психологического воздействия на человека, как: введение в заблуждение (обман), игра на чувствах (любви, ненависти, зависти, алчности, в том числе

и шантаж). Собственно, подобные приемы не новы и известны еще со времен глубокой древности. Остается только удивляться тому, что за истекшие тысячелетия человечество так и не научилось противостоять мошенникам и отличать правду ото лжи. Еще удивительнее то, что арсенал злоумышленников не претерпел никаких принципиальных изменений. Напротив, с развитием коммуникационных технологий их задача значительно упростилась. Общаясь по Интернет, вы не видите и не слышите своего собеседника, более того, нет никаких гарантий, что сообщение действительно отправлено тем адресатом, имя которого стоит в заголовке. Атакующий может находиться и в соседней комнате, и в соседнем городе, и даже на соседнем континенте! Все это значительно усложняет идентификацию личности, поиск и доказательство причастности злоумышленника к атаке. Стоит ли удивляться огромной популярности социальной инженерии среди молодежи?

Рисунок 12 — Статья «Краткое введение в социальную инженерию»

В статье «Краткое введение в социальную инженерию» [12] (рисунок 12) автор даёт понятие информации с точки зрения компании и рассматривает очень важную вещь для обеспечения безопасности – это человеческий фактор. Информация является одним из важнейших активов компании. Информация может составлять коммерческую тайну компании, т.е. при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг

или принести иную коммерческую выгоду компании. Соответственно, такую информацию необходимо защищать. Поскольку в любой компании работают люди, то неизбежно возникает влияние человеческого фактора на все процессы организации. В том числе и на процесс защиты конфиденциальной информации. Человеческий фактор — устойчивое выражение, которым обозначают психические способности человека как потенциальный и актуальный источник (причину) информационных проблем при использовании этим человеком современных технологий. Также автор рассматривает различные техники социальной инженерии, такие как:

- Претекстинг — это действие, отработанное по заранее составленному сценарию (претексту). В результате цель (жертва) должна выдать определённую информацию, или совершить определённое действие.
- Фишинг — техника, направленная на жульническое получение конфиденциальной информации.
- Троянский конь: Эта техника эксплуатирует любопытство, либо алчность цели. Злоумышленник отправляет e-mail, содержащий во вложении важное обновление антивируса, или даже свежий компромат на сотрудника.
- Дорожное яблоко: Этот метод атаки представляет собой адаптацию троянского коня, и состоит в использовании физических носителей.
- Кви про кво: Злоумышленник может позвонить по случайному номеру в компанию, и представиться сотрудником техподдержки, опрашивающим, есть ли какие-либо технические проблемы.
- Целью обратной социальной инженерии является заставить цель саму обратиться к злоумышленнику за «помощью».

Хотя термин социальной инженерии появился не так давно, сам метод получения информации таким способом используется довольно долго. Сотрудники ЦРУ и КГБ, которые хотят заполучить некоторую государственную тайну, политики и кандидаты в депутаты, да и мы сами, при желании получить что-либо, часто даже не понимая этого, используем методы социальной инженерии. Для того, чтобы обезопасить себя от воздействия социальной

инженерии, необходимо понять, как она работает. Именно поэтому автор статьи «Социальная инженерия – как не стать жертвой» [24] (рисунок 13) делает упор в сторону именно защиты от подобного психологического воздействия на человека.

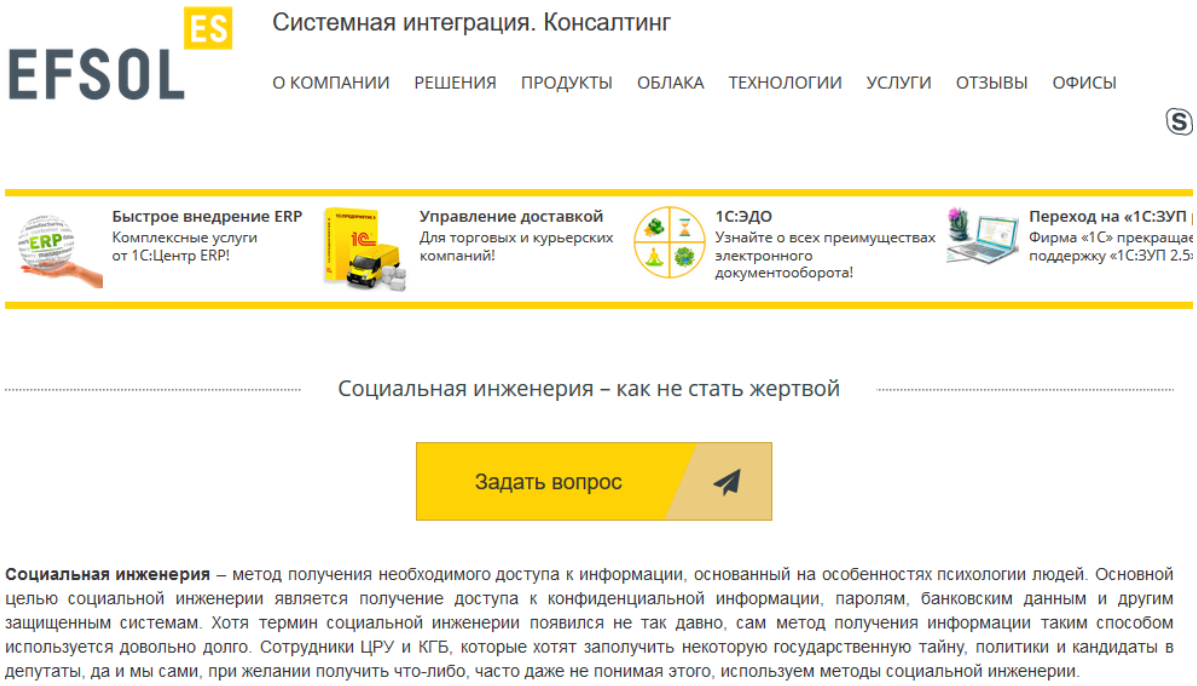

Рисунок 13 — Статья «Социальная инженерия – как не стать жертвой»

С момента появления компьютеров и начала развития Интернета программисты всеми силами стремятся обеспечить компьютерную безопасность. Но даже сегодня добиться этого на 100% не удалось никому. Однако давайте представим, что этот результат все же достигнут благодаря мощнейшей криптографии, усиленным протоколам безопасности, надежному программному обеспечению и другим элементам защиты. В итоге мы получаем абсолютно безопасную сеть и можем смело в ней работать. «Прекрасно! – скажете вы, – дело в шляпе!», но окажетесь неправы, ведь этого недостаточно. Почему? Да потому что пользу от любой компьютерной системы можно получить лишь при участии пользователей, т.е. людей. И как раз это взаимодействие между компьютером и человеком несет в себе серьезную опасность, и человек зачастую оказывается наиболее слабым звеном в цепи мер безопасности. К тому же он сам и является причиной, по которой безопасность ока-

зывается неэффективной. И поэтому в данной статье автор рассматривает то, что в информационный век манипулировать людьми стало проще, ведь есть Интернет и мобильная связь, которые позволяют взаимодействовать без непосредственного контакта. Существуют даже специальные методы, помогающие злоумышленникам «оперировать» людьми так, как им хочется. Их комплекс называется социальной инженерией, и в статье «Социальная инженерия» [25] (рисунок 14) мы попробуем выяснить, что же это такое.

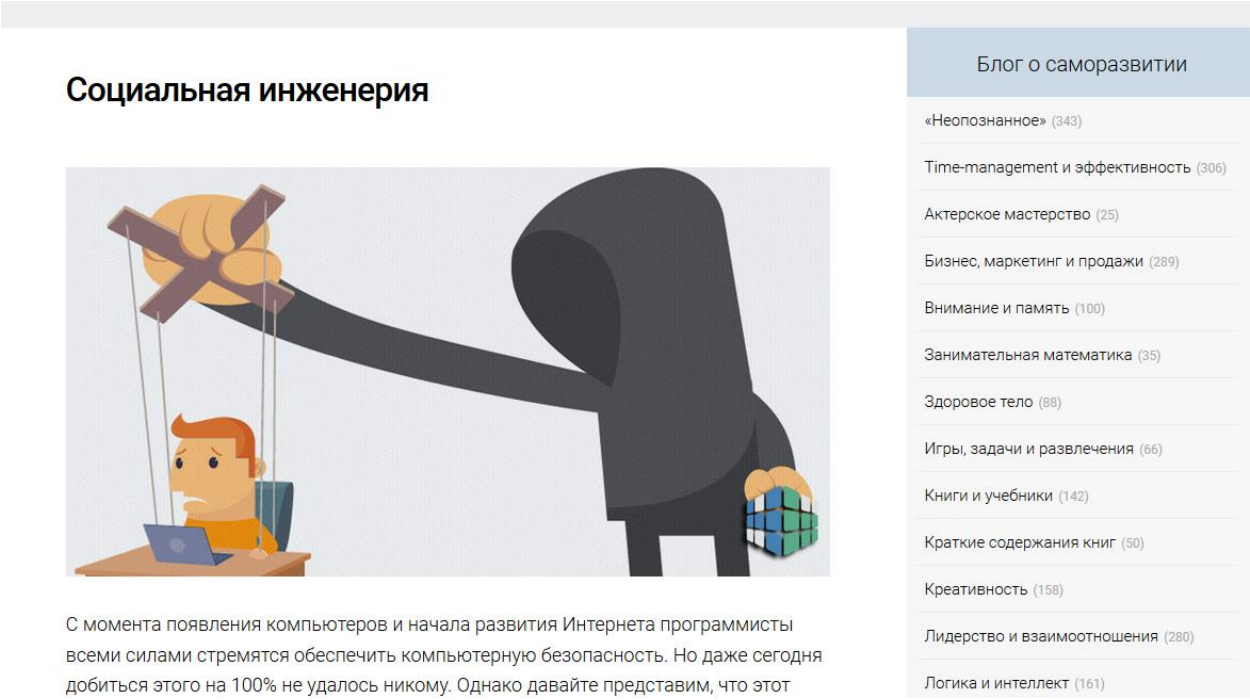

Рисунок 14 — Статья «Социальная инженерия»

1.3 Анализ рабочей программы по дисциплине «Информационная безопасность и защита информации»

Цель освоения дисциплины «Информационная безопасность и защита информации» у обучающихся по направлению документоведение и архивоведение: формирование у студентов профессиональных знаний и умений, связанных с использованием методов защиты информации и способов организации информационной безопасности на предприятии; приобретении студентами актуальных знаний и умений, позволяющих проявить себя в будущей профессиональной деятельности, реализовать свой творческий потенци-

ал путем использования существующего программного обеспечения, а так же поиска новых, более эффективных и функциональных средств защиты информации.

Задачи:

- овладение теорией и методологией защиты информации;
- приобретение знаний и умений по организационному обеспечению информационной безопасности;
- обретение основ инженерно-технической защиты информации и криптографических методов;
- ознакомление с правовой базой и законодательством российской федерации в области защиты информации.

Дисциплина направлена на формирование следующих компетенций:

- ОК-10 (способность к использованию основных методов, способов и средств получения, хранения, переработки информации);
- ОПК-6 (способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности).

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

З1. теорию информационной безопасности, методологию защиты информации;

З2. правовое обеспечение информационной безопасности, законодательную базу, систему государственного контроля и управления в области информационной безопасности;

З3. организационное обеспечение информационной безопасности;

З4. основные программные средства защиты информации;

З5. криптографические методы и средства обеспечения информационной безопасности.

Уметь:

У1. оценивать состояние организационной защиты информации на объекте;

У2. определять рациональные меры по обеспечению организационной защите на объекте;

У3. организовать работу с персоналом с секретной (конфиденциальной) информацией.

Владеть:

В1. методами выявления угроз информационной безопасности объекта;

В2. способами обеспечения режима и секретности на объекте.

Данный демонстрационный материал относится ко второму разделу «Угрозы информационной безопасности на предприятии».

В данный раздел входят следующие темы: виды угроз информационной безопасности и их характеристика. Социальная инженерия. Модели нарушителей информационной безопасности на предприятии. Формы преступного посягательства. Оценка ущерба вследствие организационных нарушений информационной безопасности на предприятии.

На данный раздел выделяется 28 часов из которых 9 часов – лекции, 8 часов – лабораторные работы, 11 часов – самостоятельная работа.

1.4 Анализ источников по формированию интерфейса для демонстрационного материала

1.4.1 Анализ литературы по интерактивному обучению

Стандартная или пассивная модель обучения использовалась в учебных заведениях с давних пор. Самый простор пример данной методики – лекция. И хотя такой способ преподавания был и остается одним из самых распространенных, интерактивное обучение постепенно становится все актуальнее.

Именно поэтому в данном демонстрационном материале используются интерактивные упражнения. Они используется с целью более полного вовлечения обучающегося в образовательный процесс.

В связи с этим было принято проанализировать книги и статьи по интерактивному обучению.

В статье «Интерактивное обучение – современные методики получения знаний» [6] рассматривается такие вещи, как понятие интерактивного обучения, какие есть средства и приёмы данного обучения. Рассматриваются психолого-педагогические аспекты и условия интерактивного обучения.

Автор статьи «Интерактивное обучение: вопросы теории и практики обучения» [7] поднимает такую тему, как то, что к условиям реализации ФГОС является широкое использование в учебном процессе активных и интерактивных форм проведения занятий. Увлечь учеников своим предметом сегодня уже невозможно без применения новых интерактивных технологий, так как односторонняя коммуникация оправдана лишь в случае недостатка информации, невозможности ее получения другим способом, кроме как из рассказа учителя. Также рассматривает и даёт различные методики и приёмы интерактивного обучения.

Коротаева Е.В. в предоставленной статье «Интерактивное обучение: плюсы и минусы» [8] рассматривает относительно новое направление в образовательном процессе интерактивное обучение, его общие характеристики, особенности и дидактические возможности. Исследует учебный диалог как основа обеспечения интерактивности и методические аспекты реализации диалога на занятиях с применением информационно-компьютерных технологий.

В данной статье рассматриваются основные плюсы и минусы таких направлений интерактивного обучения, как:

- работа в группах;
- ситуационный анализ;
- проектная технология;

- решение ситуационных задач;
- тренинги;
- деловые игры;

1.4.2 Анализ литературы по HTML и CSS

Также был проведен анализ литературных источников по теме HTML и CSS, в целях дальнейшей разработке демонстрационного материала с использованием данных технологий.

Начало данной книги (рисунок 15) [20] посвящено рассмотрению базовых принципов работы интернета и веб-сайтов. В ней в популярной форме преподносятся все основы современного веб-дизайна, рассматриваются техники создания сложных интерактивных веб-страниц, работы с графикой и таблицами стилей. Представляя собой исчерпывающую инструкцию по современным веб-стандартам. Эта книга будет полезна веб-разработчику любого уровня.

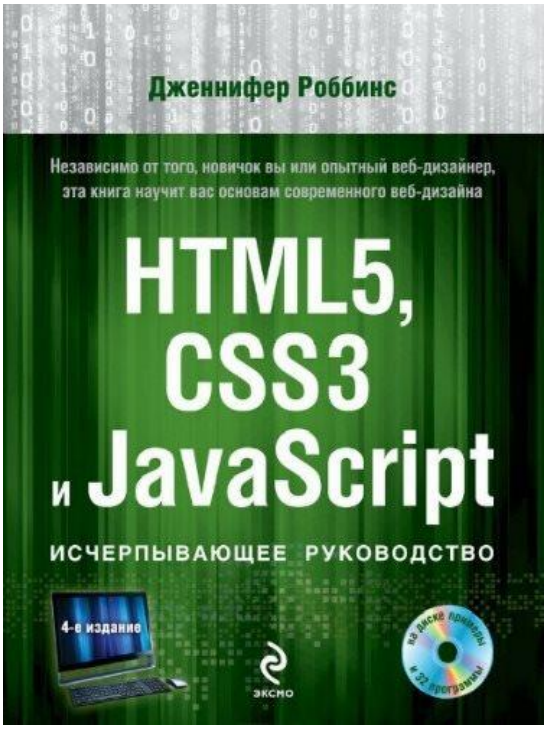

Рисунок 15 — Обложка книги «HTML5, CSS3 и JavaScript»

Веб-стандарты HTML5 и CSS3 постепенно вытесняют устаревающие технологии. Например, технологию Flash, до недавних пор весьма распространенный способ оживить веб-страницу и добавить ей интерактивности. Книга [2] рассказывает о принципах работы с векторной графикой, аудио и видео без использования Flash. Также читателю будет наглядно продемонстрировано, как хранение данных на стороне клиента в автономном режиме кэширования может кардинально улучшить скорость загрузки веб-страниц и как в этом помогают простые решения, доступные в CSS3. Каждая глава сопровождается большим количеством примеров, а также содержит задания для самостоятельного выполнения, предоставляя прекрасную возможность закрепить и упорядочить полученную информацию.

Рисунок 16 — Обложка книги «Изучаем HTML5»

Эта книга (рисунок 16) [3] посвящена изучению нового стандарта веб-программирования HTML5 и использованию новых функциональных возможностей, предоставляемых веб-разработчикам. Написанная опытными программистами, давно использующими HTML5 в своей работе, книга расскажет, как приступить к освоению этого языка программирования и адаптации веб-проектов для того, чтобы в полной мере воспользоваться преимуще-

ствами нового стандарта. Авторы не заставляют вас читать избыточно подробные спецификации языка, а учат применять HTML5 на конкретных примерах. С помощью этой книги вы узнаете, каковы новые семантики и структуры HTML5, как использовать мультимедийные элементы HTML5 для размещения аудио- и видеоданных, как разрабатывать «умные» веб-формы и усовершенствовать приложения, использующие географическую привязку, с помощью API геолокации.

«HTML и XHTML. Подробное руководство» [28] – самая полная и современная книга по языкам HTML и XHTML, разъясняющая работу и взаимодействие каждого их элемента. Она удачно сочетает в себе лучшие качества понятного учебного пособия, адресованного начинающим, и всеобъемлющего справочника, который всегда под рукой даже у опытных веб-программистов. Этот труд, ставший классическим, содержит все от базового описания синтаксиса и семантики до практических советов, поможет вам найти свой неповторимый стиль и в совершенстве овладеть языком веб-дизайна. Описаны стандарты HTML 4.01, XHTML 1.0 и CSS2, приведен обзор еще не вступивших в силу стандартов XHTML 2 и CSS3. Уделено внимание к новейшим инициативам разработчиков XHTML (XForms, XFrames и модуляризации), а также основам XML. Рассмотрены: управление внешним видом документа с помощью таблиц стилей; работа с HTML-кодом, сгенерированным автоматически; работа с фреймами, интерактивными формами, динамическими документами; интеграция HTML-кода с мультимедийными данными, сценариями JavaScript и Java-апплетами.

Это мануал [5], в котором вы найдете не так много теоретической базы – вся информация строится на реальных примерах, которые вы можете самостоятельно опробовать и посмотреть на результат. В книге рассматривается разработка сайтов на основе концепции Web 2.0. Даются описания языков HTML 5 и CSS 3, которые применяются для создания содержимого и представления веб-страниц.

Создатели этого справочника [31] постарались охватить максимальную аудиторию, сделав из книги простое и понятное пособие для новичков и настоящий кладезь информации даже для матерых верстальщиков. Как такое стало возможным? Авторы постарались дать максимально полную информацию по этим двум языкам. Начиная от самого простого базового синтаксиса и семантики до практических советов, которые можно использовать на любом уровне владения профессией.

2 ОПИСАНИЕ ДЕМОНСТРАЦИОННОГО МАТЕРИАЛА «СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ»

2.1 Педагогический адрес

Демонстрационный материал с элементами интерактивности «Социальная инженерия» предназначен для ведения лекций в рамках дисциплины «Информационная безопасность и защита информации» для обучающихся федерального государственного автономного образовательного учреждение высшего образования «Российский государственный профессионально-педагогический университет» по направлению подготовки 46.03.02 Документоведение и архивоведение.

2.2 Разработка теоретического материала

Данный демонстрационный материал делится на 4 блока:

1. Главная страница.
2. Теоретический блок.
3. Практический блок.
4. Дополнительные материалы.

Теоретический блок в свою очередь делится на 6 разделов:

1. Введение в социальную инженерию.
2. Области применения.
3. Фишинг.
4. Претекстинг.
5. Обратная социальная инженерия.
6. Способы защиты от социальной инженерии.

Такой блочный подход был выбран для более удобного поиска нужной информации, также для более комфортной работы с данным продуктом. Для

этого отдельно были вынесены материалы по теории, по практике и доп. материалы. Более подробная структура предоставлена на рисунке 17.

Рисунок 17 — Структура продукта

На главной странице содержится аннотация, которая включает в себя краткую характеристику предоставленного демонстрационного материала.

В практическом блоке собраны различные интерактивные приложения, направленные на непосредственное вовлечение обучающихся в образовательный процесс за счёт использования современных интерактивных технологий, например таких как интерактивная доска.

В блоке дополнительных материалов собраны различные видеоматериалы по теме «Социальная инженерия», которые очень хорошо дополняют содержание презентаций и демонстрируют современный мультимедийный подход к образовательному процессу.

2.3 Методические указания к демонстрационному материалу

Данный материал был разработан для использования педагогом во время проведения лекций. Так как объём учебного материала превышает часы, выделенные на изучение данной темы, то по усмотрению преподавателя некоторые темы могут быть вынесены на самостоятельное обучение.

2.4 Описание выбранных технологий для написания интерфейса демонстрационного материала

Для укомплектования всего материала в более удобную и доступную форму был выбран язык гипертекстовой разметки (HTML – стандартизированный язык разметки документов во Всемирной паутине) и каскадные таблицы стилей (CSS – формальный язык описания внешнего вида документа, написанного с использованием языка разметки).

Для более простой работы в HTML и CSS был выбран визуальный HTML-редактор Notepad++ (рисунок 18).

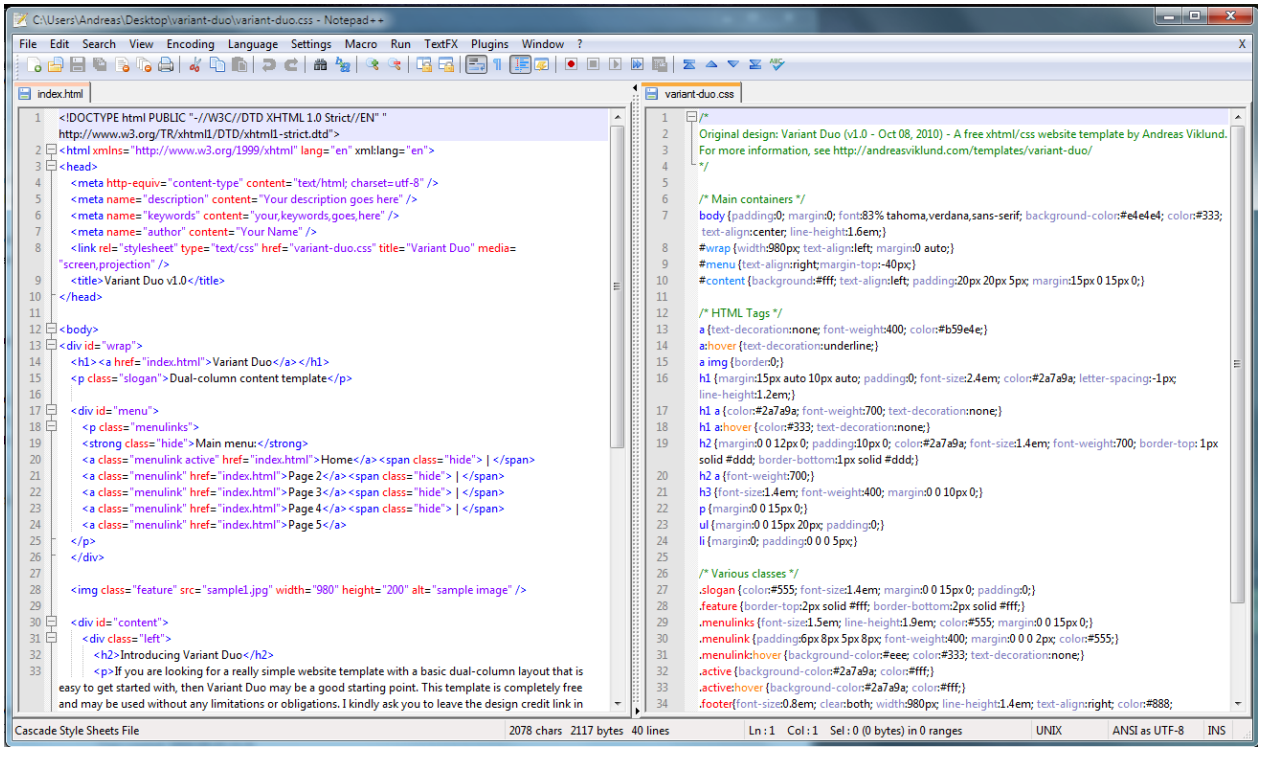

Рисунок 18 — Интерфейс Notepad++

Notepad++ – свободный текстовый редактор с открытым исходным кодом для Windows, с подсветкой синтаксиса большого количества языков программирования и разметки. Поддерживает открытие более 100 форматов. Базируется на компоненте Scintilla, написан на C++ с использованием STL, а также Windows API и распространяется под лицензией GNU General Public License. Базовая функциональность программы может быть расширена как за счёт плагинов, так и сторонних модулей, таких как компиляторы и препроцессоры.

Для предоставления демонстрационного материала был выбран MS PowerPoint (рисунок 19).

Microsoft PowerPoint – программа подготовки презентаций и просмотра презентаций, являющаяся частью Microsoft Office и доступная в редакциях для операционных систем Microsoft Windows и macOS. Материалы, подготовленные с помощью PowerPoint предназначены для отображения на большом экране – через проектор, либо телевизионный экран большого размера.

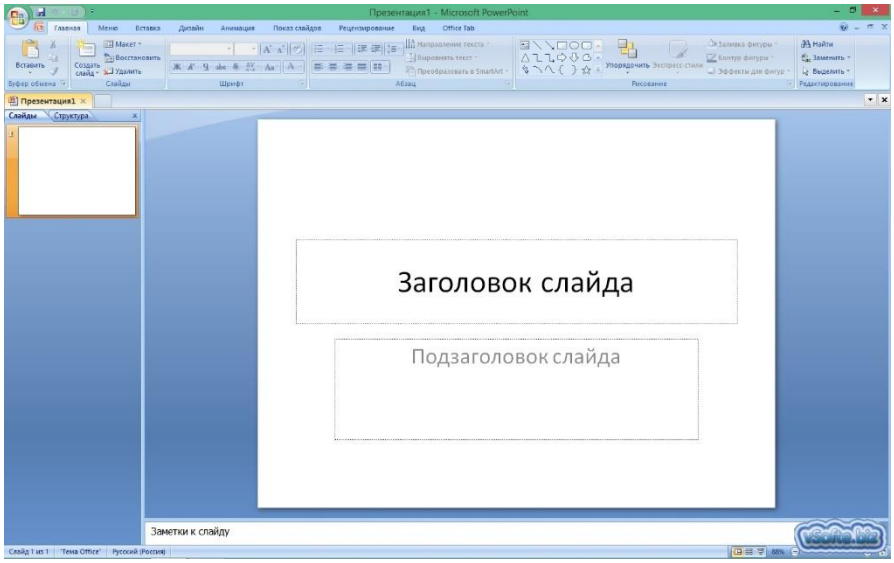

Рисунок 19 — Интерфейс MS PowerPoint

Также были разработаны интерактивные упражнения для использования на лекции, при наличии интерактивной доски. Данные упражнения были разработаны на ресурсе learningapps (рисунок 20).

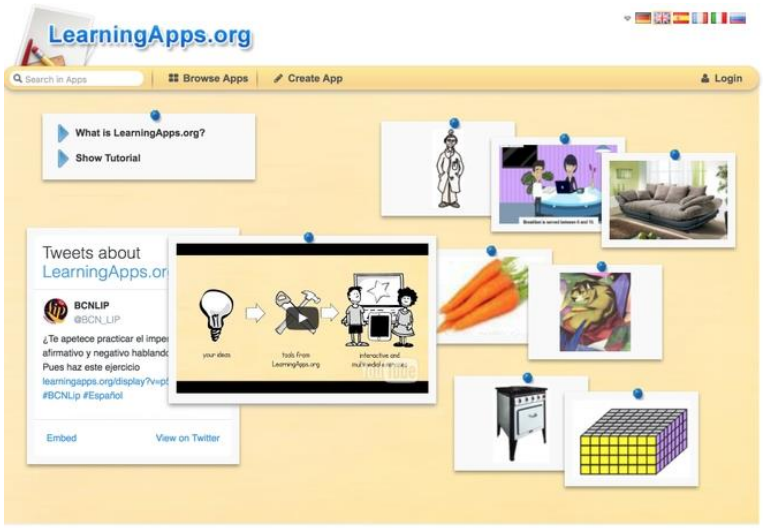

Рисунок 20 — Интерфейс learningapps

LearningApps – это ресурс для поддержки учебного процесса с помощью интерактивных модулей (приложений, упражнений). Данный онлайн-ресурс позволяет создавать такие модули, сохранять и использовать их, обеспечивать свободный обмен ими между педагогами, организовывать работу обучающихся (в том числе, и по созданию новых модулей). Также он является полностью бесплатным. Был разработан в Германии

2.5 Описание интерфейса демонстрационного материала

Содержание демонстрационного материала структурировано, информация тщательно подобрана и разбита на 4 основных блока. Оформление соответствует задаваемой тематике и придерживается корпоративных цветов вуза, так как данный продукт разрабатывается для дисциплины, которая будет читаться в РГППУ.

Разработка данного продукта выполнялась поэтапно:

- анализ литературы по теме;
- сбор и структурирование материалов по теме;
- разработка демонстрационного материала;
- разработка интерфейса демонстрационного материала;
- проверка продукта на работоспособность;

- исправление ошибок.

Начальная страница разработанного интерфейса демонстрационного материала представлена на рисунке 21.

Рисунок 21 — Начальная страница

На главной странице продукта можно изучить краткую характеристику данного демонстрационного материала.

Также в меню наверху можно увидеть основные разделы продукта.

Данный демонстрационный материал разработан для обучающихся по направлению подготовки 46.03.02 Документоведение и архивоведение. Российского государственного профессионально-педагогического университета, и читается в рамках дисциплины «Информационная безопасность и защита информации».

Для открытия демонстрационного материала следует выполнить двойной клик левой кнопкой мыши по файлу index.html. После этого на экране откроется главная страница (рисунок 21).

Навигация по сайту осуществляется довольно просто. В верхней части окна располагается меню, в котором указаны все блоки данного продукта. Это сделано для удобного перемещения между нужными отделами.

На рисунке 22 продемонстрирована панель навигации

Рисунок 22 — Панель навигации

Меню содержит следующие разделы:

1. Главная страница.
2. Лекционный материал.
3. Упражнения.
4. Дополнительный материал.

Также было сделано не слишком большее цветовое разнообразие, в целях меньшего отвлечения обучающегося от образовательного процесса. Текст был выбран чёрного цвета, в целях его читабельности при показе на интерактивной доске.

2.6 Описание демонстрационного материала

2.6.1 Описание презентаций

Демонстрационный материал предоставлен в виде презентаций (рисунок 23). Это делается с целью большей наглядности в образовательном процессе. Также посредством презентации можно скомпоновать довольно большой объём информации в строгий и структурированный доклад, который будет довольно прост и удобен в предоставлении материала обучающимся. В данном виде подаче материала педагог может сосредоточить внимание на самых важных моментах, особо не рассеивая внимание на не особо важные пункты изложения материала.

На сайте можно просмотреть все презентации, но для удобства и с целью использования всех интерактивных возможностей презентации необходимо её скачать. Ссылка на скачивание находится под презентацией.

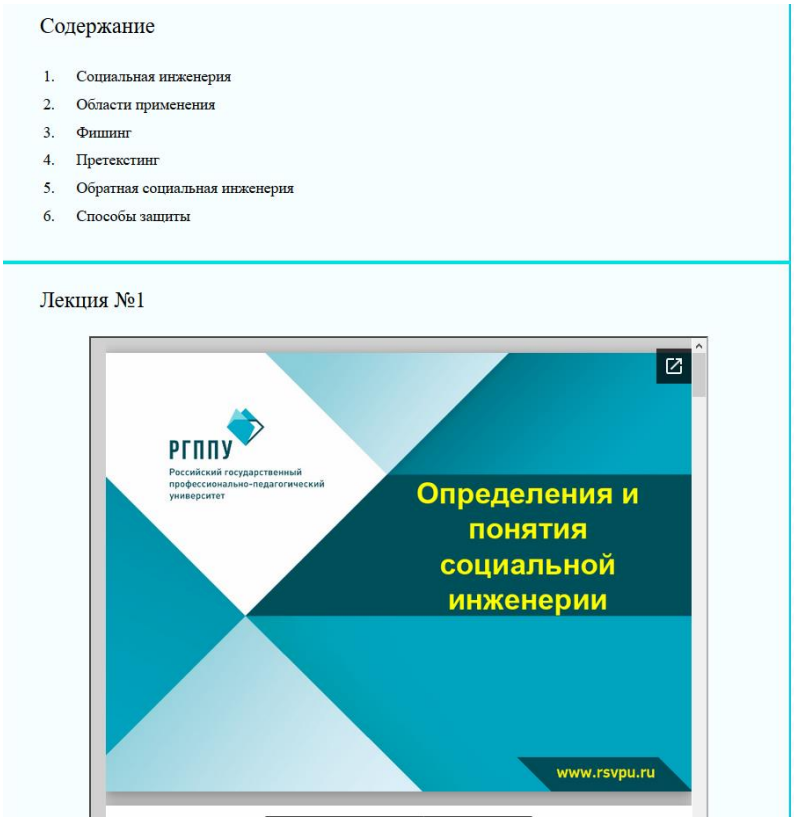

Рисунок 23 — Страница «Теория»

Презентация №1 «Введение в социальную инженерию».

В данной презентации (рисунок 24) даются основные понятия и определения в сфере социальной инженерии.

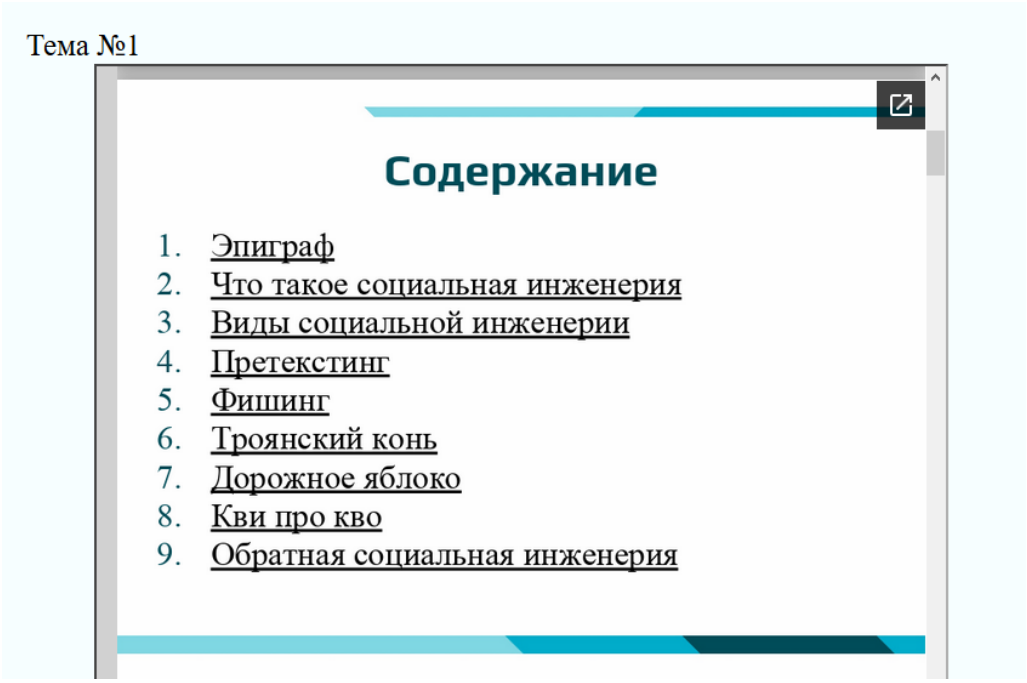

Рисунок 24 — Презентация «Введение в социальную инженерию»

Презентация №2 «Области применения СИ».

В данной презентации (рисунок 25) рассматриваются история возникновения социальной инженерии и основные области применения социальной инженерии с примерами использования в этих областях.

Рисунок 25 — Презентация «Области применения СИ»

Презентация №3 «Фишинг».

В данной презентации (рисунок 26) изучается такая техника социальной инженерии, как фишинг. Даются знания о том, что такое фишинг и в чём его особенности.

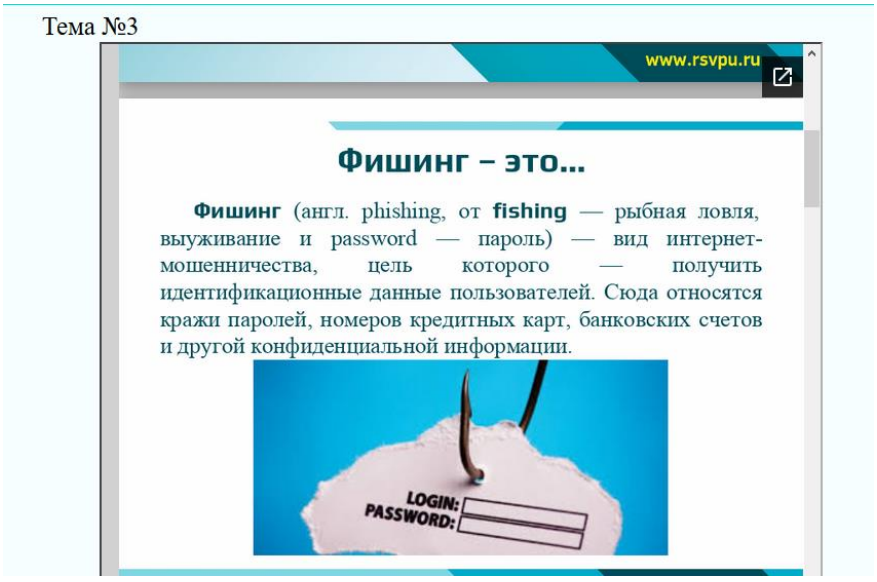

Рисунок 26 — Презентация «Фишинг»

Презентация №4 «Претекстинг».

В данной презентации (рисунок 27) изучается такая техника социальной инженерии, как претекстинг.

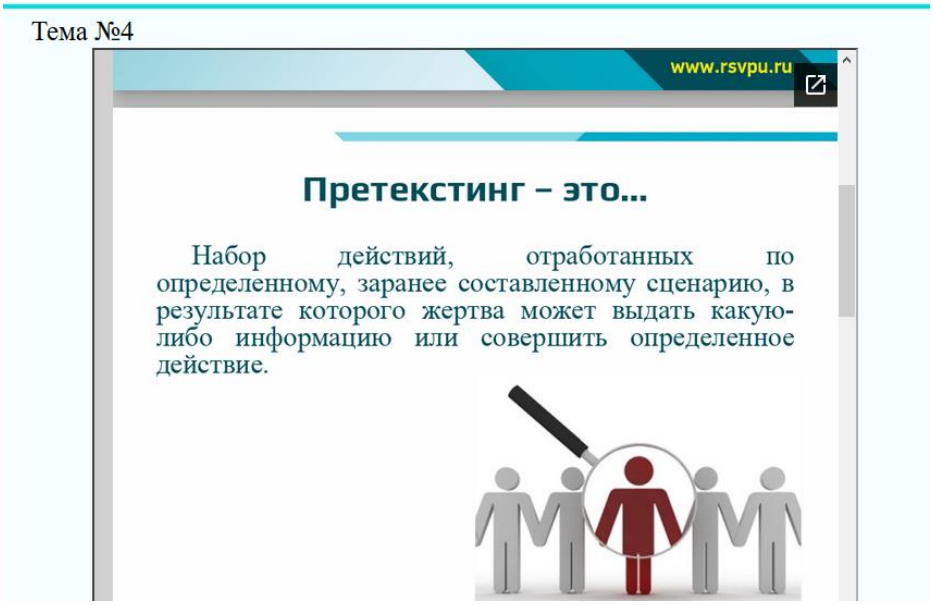

Рисунок 27 — Презентация «Претекстинг»

Презентация №5 «Обратная социальная инженерия».

В данной презентации (рисунок 28) рассматривается такое понятие, как обратная социальная инженерия, в чём её особенности и в чём различие между социальной инженерией.

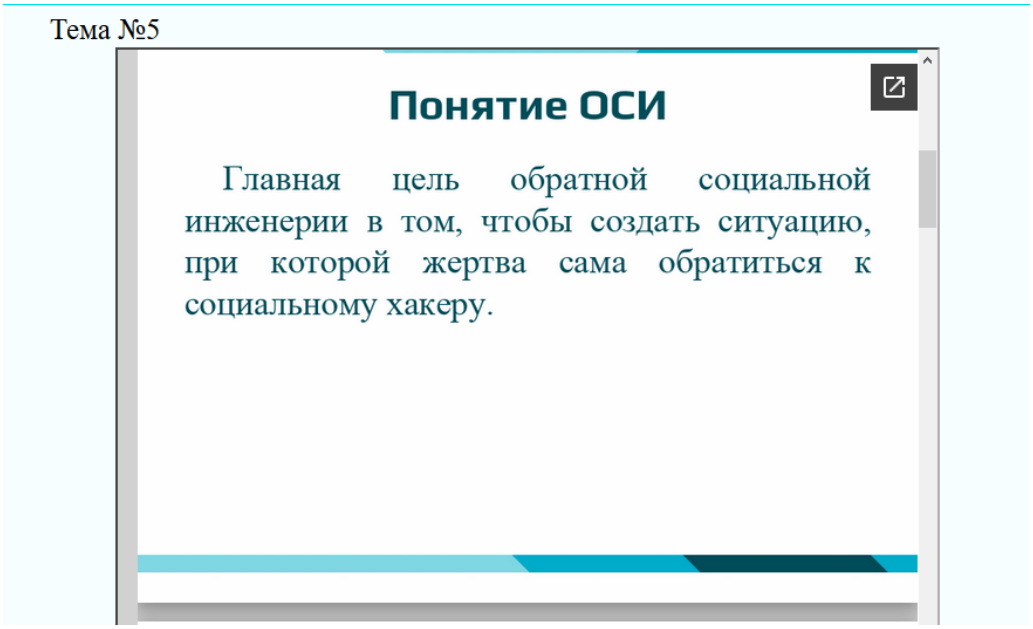

Рисунок 28 — Презентация «Обратная социальная инженерия»

Презентация №6 «Способы защиты от социальной инженерии»

В данной презентации (рисунок 29) собраны основные методы защиты от СИ.

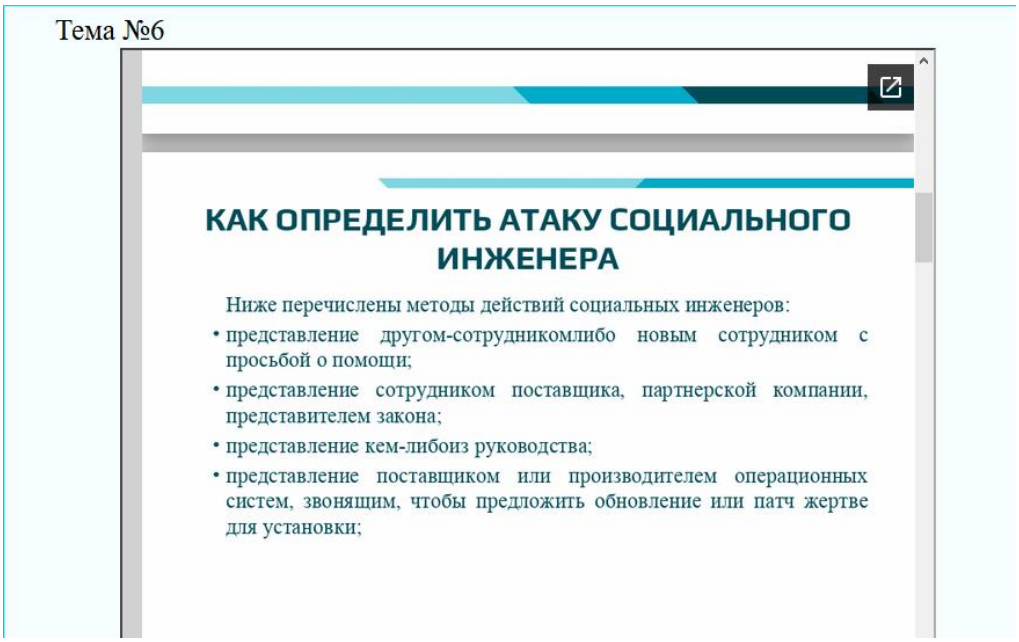

Рисунок 29 — Презентация «Способы защиты от социальной инженерии»

Все презентации выполнены учитывая требования создания презентаций и предоставления информации. Также они все выполнены в корпоративных цветах РГППУ. Так как демонстрационный материал разрабатывался для дисциплины, которая изучается в данном образовательном учреждении.

Для более удобного перемещения по странице с теорией были сделаны гиперссылки.

Также сделаны перекрёстные ссылки между разделом с упражнениями, для более удобного и быстрого использования всех возможностей данного продукта.

2.6.2 Упражнения

В качестве средства для закрепления материала были выбраны интерактивные упражнения, которые позволят разнообразить и улучшить образовательный процесс непосредственно вовлекая в него обучающихся.

Ведь именно интерактивный подход к образовательному процессу даёт возможность вовлечения каждого участника, позволяет построить диалогичность общения между педагогом и обучающимися и даёт очень хорошую площадку для дальнейшей рефлексии. Данные интерактивные упражнения можно использовать как для самостоятельного контроля обучающегося, так и на лекции, если имеется интерактивная доска.

Платформой для создания интерактивных упражнений был выбран ресурс learningapps. Данный ресурс очень удобен в использовании и является бесплатным. На данном ресурсе можно разрабатывать интерактивные задания и в последствии рассылать их обучающимся или закрепить на своем сайте/блоге/ресурсе.

Упражнение № 1.

В данном упражнении необходимо соотнести определение с его расшифровкой (рисунок 30).

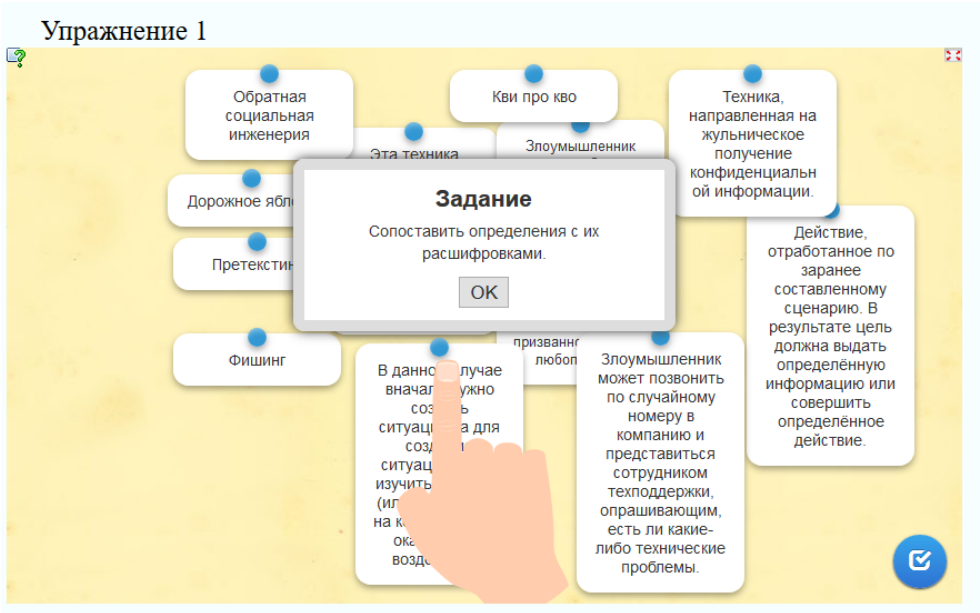

Рисунок 30 — Упражнение 1

Упражнение №2.

В данном упражнении необходимо распределить по группам различные виды социальной инженерии (рисунок 31).

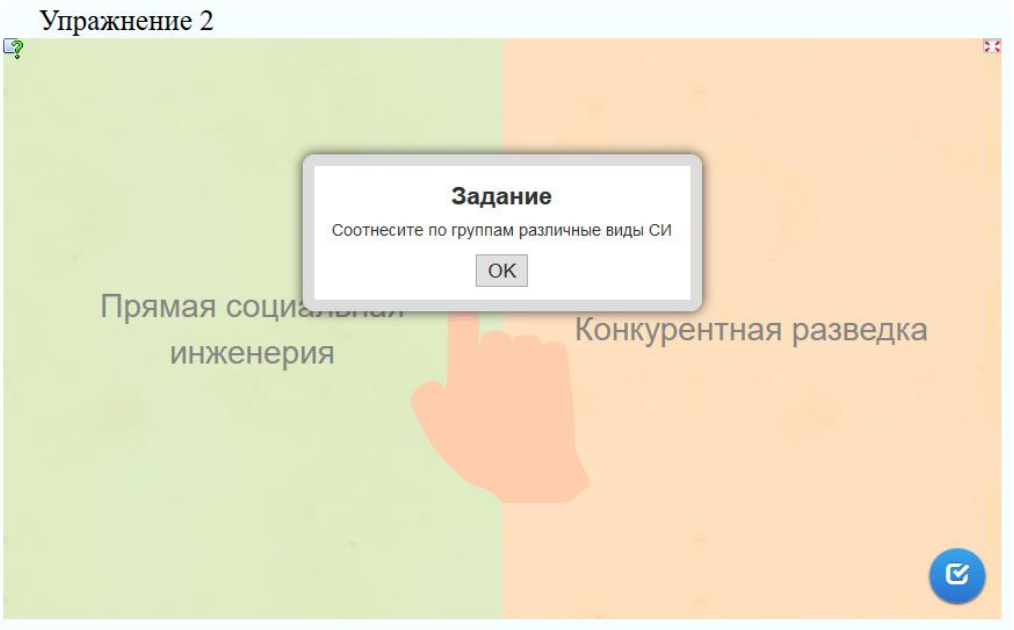

Рисунок 31 — Упражнение 2

Упражнение №3.

В данном упражнении дан текст по теме «Новые угрозы в сфере социальная инженерия». В этом тексте необходимо заполнить пропуски (рисунок 32).

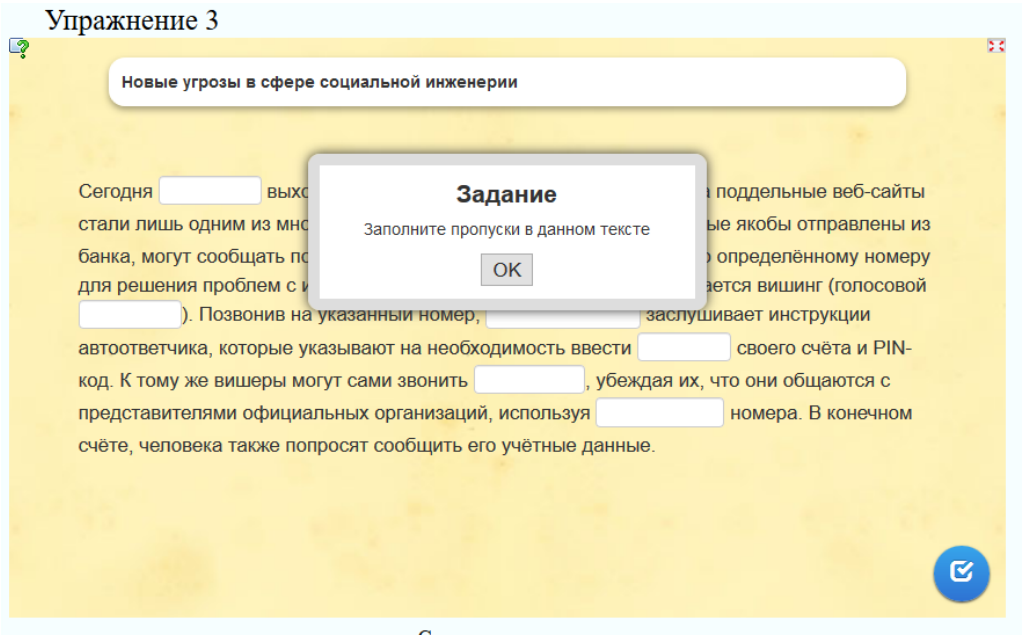

Рисунок 32 — Упражнение 3

Упражнения №4.

В данном упражнении посредством игры «Виселица» идёт повторение и закрепление терминов в области социальной инженерии (рисунок 33).

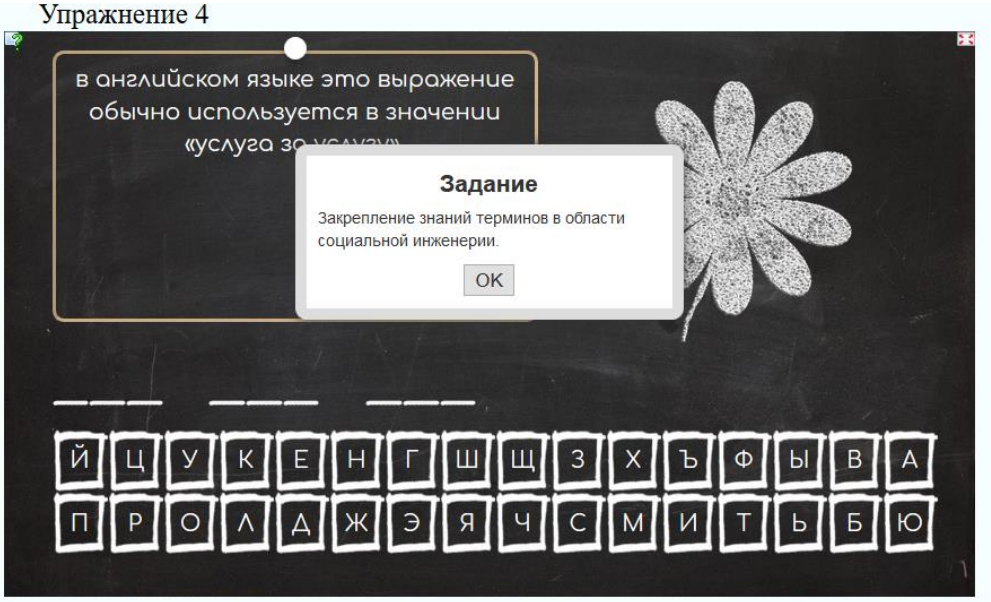

Рисунок 33 — Упражнение 4

Упражнение №5

В данном упражнении необходимо отыскать нужное количество слов из сферы социальная инженерия (рисунок 34).

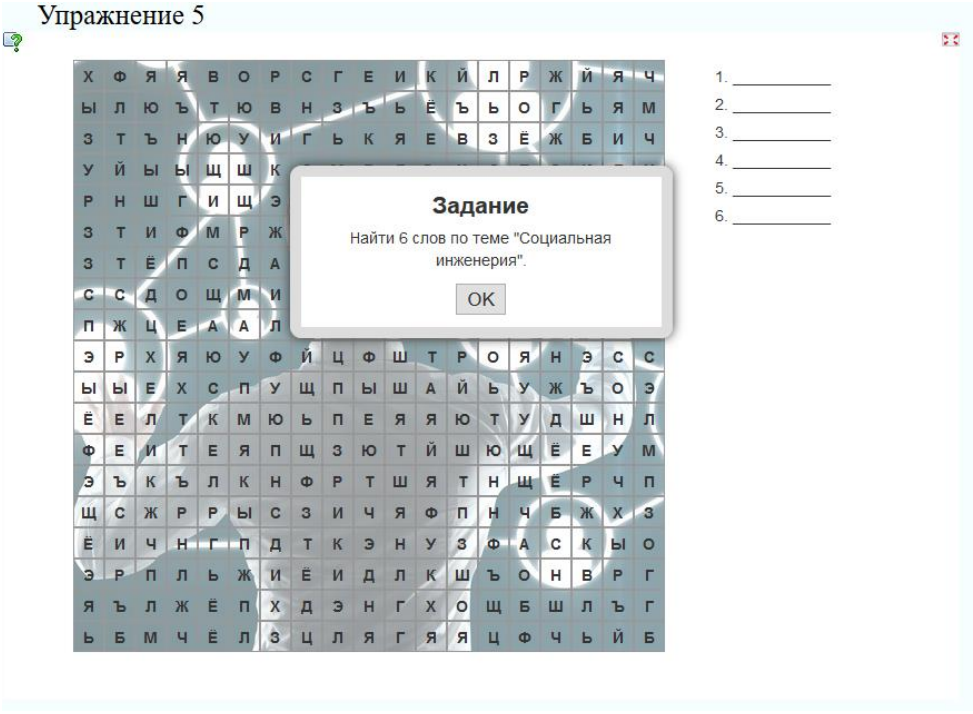

Рисунок 34 — Упражнение 5

Упражнения выполняются после изучения теоретического материала. По средствам этих упражнений обучающиеся вспоминают и закрепляют весь пройденный материал.

2.6.3 Дополнительные материалы

В дополнительных материалах собраны видео по теме «Социальная инженерия» (рисунок 35), которые являются очень хорошим дополнением к теоретическому материалу.

Видеоматериалы были тщательно подобраны и несут в себе цель разнообразия образовательного процесса по средствам мультимедийных технологий.

Видеоматериалы были взяты из открытых источников и обеспечивают максимальную наглядность.

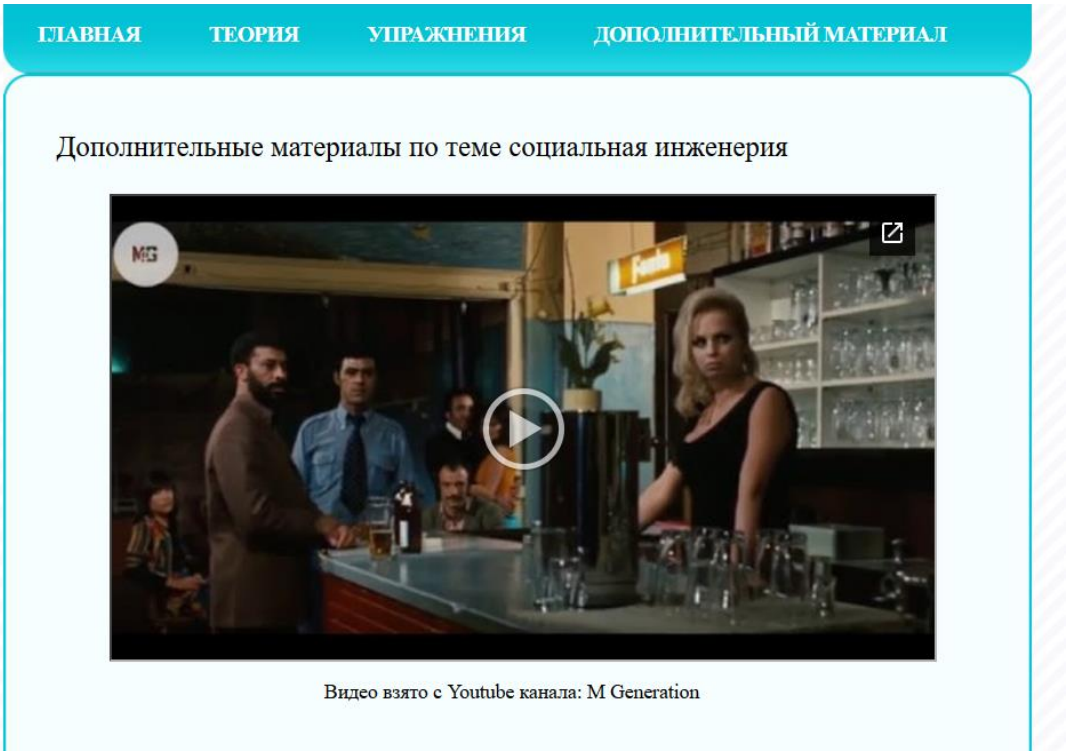

Рисунок 35 — Страница дополнительного материала

ЗАКЛЮЧЕНИЕ

В рамках выпускной квалификационной работы был разработан демонстрационный материал с элементами интерактивности для обучающихся Российского государственного профессионально-педагогического университета по направлению подготовки 46.03.02 Документоведение и архивоведение, и используется в рамках дисциплины «Информационная безопасность и защита информации».

При выполнении выпускной квалификационной работы были решены следующие задачи:

1. Был проведен анализ различных печатных и интернет-источников по теме «Социальная инженерия».
2. Проведен анализ учебной программы по дисциплине «Информационная безопасность и защита информации».
3. Проанализирована литература по интерактивному обучению.
4. Также изучены источники литературы по html и css.
5. Собран и структурирован материал по теме «Социальная инженерия».
6. Разработаны презентации и интерактивные упражнения по теме.
7. Демонстрационный материал реализован в электронном виде с помощью html и css и содержит в себе:

- аннотацию;
- теоретический материал, предоставленный в виде презентаций;
- интерактивные приложения;
- дополнительный материал.

При разработке демонстрационного материала были использованы такие технологии как язык гипертекстовой разметки HTML, CSS, визуальный HTML-редактор Notepad, для создания презентаций был использован MS

PowerPoint, интерактивные приложения были разработаны в ресурсе под названием learningapps.

Таким образом, поставленные задачи можно считать выполненными в полном объеме, а цель достигнутой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Альфред Адлер Понять природу человека [Текст] / Альфред Адлер — Санкт-Петербург: Академический Проект, 1997. — 256 с.
2. Брайн Хоган HTML5 и CSS3. Веб-разработка по стандартам нового поколения [Текст] / Хоган Брайн — Санкт-Петербург: Питер, 2012. — 272 с.
3. Брюс Лоусон Изучаем HTML5 [Текст] / Брюс Лоусон, Реми Шарп — пер. с англ. Т. Качковская, Е. Шикарева — Санкт-Петербург: Питер, 2011. — 272 с.
4. Брюс Шнейер Секреты и ложь. Безопасность данных в цифровом мире [Текст] / Шнейер Брюс — пер. с англ. Н. Дубнова — Санкт-Петербург: Питер, 2003. — 368 с.
5. Владимир А.Д. HTML 5, CSS 3 и Web 2.0. Разработка современных Web-сайтов [Текст] / А.Д. Владимир — Санкт-Петербург: БХВ-Петербург, 2011. — 416 с.
6. Интерактивное обучение – современные методики получения знаний [Электронный ресурс] — Режим доступа — https://womanadvice.ru/interaktivnoe-obuchenie-sovremennye-metodiki-polucheniya-znaniy (дата обращения: 01.06.2018).
7. Интерактивное обучение: вопросы теории и практики обучения [Электронный ресурс] — Режим доступа — https://cyberleninka.ru/article/n/interaktivnoe-obuchenie-voprosy-teorii-i-praktiki-obucheniya (дата обращения: 01.06.2018).
8. Интерактивное обучение: плюсы и минусы [Электронный ресурс] — Режим доступа — https://www.mindmeister.com/ru/280004690/_ (дата обращения: 01.06.2018).
9. Кевин Митник Искусство вторжения [Текст] / Вильям Л. Саймон, Кевин Митник — пер. с англ. Семенов А.В. — Москва: Компания АйТи, 2005. — 280 с.

10. Кевин Митник Искусство обмана [Текст] / Вильям Л. Саймон, Кевин Митник — пер. с англ. Груздев А.А., Семенов А.В. — Москва: Компания АйТи, 2004. — 360 с.

11. Кевин Митник Призрак в сети [Текст] / Вильям Л. Саймон, Кевин Митник — пер. с англ. Семенов А.В. — Москва: Эксмо, 2017. — 416 с.

12. Краткое введение в социальную инженерию [Электронный ресурс] — Режим доступа — https://habr.com/post/83415/ (дата обращения: 01.06.2018).

13. Кузнецов М.В. Социальная инженерия и социальные хакеры [Текст] / М.В. Кузнецов, И.В. Симдянов — Санкт-Петербург: БХВ, 2007. — 358 с.

14. Определение понятия социальной инженерии и её наполнения [Электронный ресурс] — Режим доступа — http://soc.bobrodobro.ru/16999 (дата обращения: 01.06.2018).

15. Официальный сайт Сибайского института (филиала) БашГУ [Электронный ресурс] — Режим доступа — http://www.sibsu.ru/ (дата обращения: 01.06.2018).

16. Подборка материалов по HTML и CSS [Электронный ресурс] — Режим доступа — https://proglib.io/p/html-css-collection/ (дата обращения: 01.06.2018).

17. Пол Экман Психология лжи. Обмани меня, если сможешь [Текст] / Пол Экман — пер. с англ. Н. Исупова, Н. Мальгина, О. Терехова, Н. Миронов — Санкт-Петербург: Питер, 2016. — 384 с.

18. РГППУ Российский государственный профессионально-педагогический университет в Екатеринбурге [Электронный ресурс] — Режим доступа — http://www.rsvpu.ru/ (дата обращения: 01.06.2018).

19. Реферат: Понятия социальная инженерия [Электронный ресурс] — Режим доступа — https://www.bestreferat.ru/referat-325148.html (дата обращения: 01.06.2018).

20. Роббинс Дженнифер HTML5, CSS3 и JavaScript исчерпывающее руководство [Текст] / Дженнифер Роббинс — пер. с англ. М.А. Райтман — Москва: Эксмо, 2014. — 528 с.

21. Робер Чалдин Психология влияния [Текст] / Роберт Чалдин — пер. с англ. Е. Бугаева, Е. Волков, Ирина Волкова, О. Пузырева — Санкт-Петербург: Питер, 2016. — 520 с.

22. СИ. Что такое социальная инженерия и методы защиты [Электронный ресурс] — Режим доступа — https://pikabu.ru/story/si_chto_takoe_sotsialnaya_inzheneriya_i_metodyi_zashchityi_5137593 (дата обращения: 01.06.2018).

23. Социальная инженерия для начинающих – методы и приемы, социальная инженерия как наука [Электронный ресурс] — Режим доступа — https://womanadvice.ru/socialnaya-inzheneriya-kak-ne-popastsya-na-udochku-moshennikam (дата обращения: 01.06.2018).

24. Социальная инженерия – как не стать жертвой [Электронный ресурс] — Режим доступа — http://efsol.ru/articles/social-engineering.html (дата обращения: 01.06.2018).

25. Социальная инженерия [Электронный ресурс] — Режим доступа — https://4brain.ru/blog/%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F-%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F/ (дата обращения: 01.06.2018).

26. Социальная инженерия, или, как «взломать» человека [Электронный ресурс] — Режим доступа — https://www.kaspersky.ru/blog/socialnaya-inzheneriya-ili-kak-vzlomat-cheloveka/2559/ (дата обращения: 01.06.2018).

27. Хенрик Фексеус Искусство манипуляции. Как читать мысли других людей и незаметно управлять ими [Текст] / Хенрик Фексеус — пер. с англ. Хохлова Е. — Москва: АСТ, 2015. — 190 с.

28. Чак Маскиано HTML и XHTML. Подробное руководство [Текст] / Чак Маскиано, Бил Кеннеди — пер. с анг. С. Иноземцев — Москва: Символ-Плюс, 2011. — 752 с.

29. Что такое «фишинг» [Электронный ресурс] — Режим доступа — https://securelist.ru/threats/chto-takoe-fishing/ (дата обращения: 01.06.2018).

30. Эрик Берн Игры, в которые играют люди. Психология человеческих взаимоотношений [Текст] / Эрик Берн — пер. с англ. А. Грузберг — Москва: Эксмо, 2017. — 352 с.

31. HTML-тэги – полный список [Электронный ресурс] — Режим доступа — https://html5book.ru/html-tags/ (дата обращения: 01.06.2018).

32. PSYCHO: Социальный инженер – всем хакерам пример [Электронный ресурс] — Режим доступа — https://xakep.ru/2010/12/15/54169/ (дата обращения: 01.06.2018).

ПРИЛОЖЕНИЕ

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий
направление 44.03.04 Профессиональное обучение (по отраслям)
профиль «Информатика и вычислительная техника»
профилизация «Информационная безопасность»

УТВЕРЖДАЮ
Заведующий кафедрой
_____Н. С. Толстова
«_____»_____2018 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студента 4 курса, ИБ-401 Климчика Александра Максимовича

1. Тема Демонстрационный материал с элементами интерактивности «Социальная инженерия»
утверждена распоряжением по институту от 25.12.2017 г. №

2. Руководитель Окуловская Анастасия Георгиевна, старший преподаватель

3. Место преддипломной практики ФГАОУ ВО «Российский государственный профессионально-педагогический университет»
4. Исходные данные к ВКР

Кевин Митник Искусство обмана [Текст] / Вильям Л. Саймон, Кевин Митник — пер. с англ. Груздев А.А., Семенов А.В. — Москва: Компания АйТи, 2004. — 360 с.
5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)

Анализ литературы и интернет-источников.
Анализ рабочей программы.
Анализ источников по формированию интерфейса для демонстрационного материала
Разработка демонстрационный материал с элементами интерактивности «Социальная инженерия»

6. Перечень демонстрационных материалов
Презентация, выполненная в Microsoft PowerPoint, продукт в форме локального сайта, выполненный на HTML, демонстрационный материал, выполненный в MS PowerPoint, интерактивные упражнения, выполненные в LearningApps.org.

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной квалификационной работе	23.04.2018	15%	подпись
2	Выполнение работ по разрабатываемым вопросам и их изложение в пояснительной записке:		65%	подпись
2.1	Анализ литературных и интернет источников	27.05.2018	10%	подпись
2.2	Анализ учебной документации по дисциплинам	03.06.2018	10%	подпись
2.3	Разработка демонстрационного материала по теме	06.06.2018	20%	подпись
2.4	Разработка интерфейса лабораторного практикума	07.06.2018	25%	подпись
3	Оформление текстовой части ВКР	08.05.2018	5%	подпись
4	Выполнение демонстрационных материалов к ВКР	10.06.2018	5%	подпись
5	Подготовка доклада к защите в ГЭК	13.06.2018	5%	подпись

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

Руководитель _____ *Задание получил* _____
подпись дата подпись студента дата

9. Выпускная квалификационная работа и все материалы проанализированы.
Считаю возможным допустить Климчика А.М. к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

Руководитель _____ _____
подпись дата

10. Допустить Климчика А.М. к защите выпускной квалификационной работы в государственной экзаменационной комиссии (протокол заседания кафедры от __.__.2018 №____)

Заведующий кафедрой _____ _____
подпись дата