Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий

Прикладная математика и информатика

09.03.03 Прикладная информатика

Бизнес-информатика

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему «Разработка проекта внедрения системы корпоративного обучения сотрудников Deutsche Telekom»

Студент(ка) К. В. Реус _____ _____
(И.О. Фамилия) (личная подпись)

Руководитель О. М. Гущина _____ _____
(И.О. Фамилия) (личная подпись)

Допустить к защите

Заведующий кафедрой к.т.н., доцент, А. В. Очеповский _____
(личная подпись)

«_____»_____20_____г.

Тольятти 2018

Росдистант
ВЫСШЕЕ ОБРАЗОВАНИЕ ДИСТАНЦИОННО

Аннотация

Выпускная квалификационная работа посвящена теме разработки проекта внедрения системы корпоративного обучения сотрудников Deutsche Telekom.

В работе рассматривается вопрос повышения информационной безопасности компании путём внедрения корпоративной системы обучения для предотвращения возникновения инцидентов информационной безопасности, вызванных некорректными действиями сотрудников.

Структура работы представлена введением, тремя главами, четырнадцатью параграфами, заключением, списком литературы и одним приложением. Объём работы - 62 страницы, на которых размещены 28 рисунков и 1 таблица. При написании работы использовалось несколько источников, собственные публикации отсутствуют.

Во введении описана актуальность выбранной темы, цель, задачи, а также объект и предмет исследования.

Первая глава содержит характеристику предприятия, описание процедуры предоставления доступа к конфиденциальной информации компании новым сотрудникам, выявление имеющихся недостатков в данном процессе и предложение по устранению данных недостатков.

Вторая глава содержит описание проекта внедрения и тестирования системы обучения, а также пример работы с системой.

Третья глава содержит описание экономического эффекта от внедрения системы.

Полученное решения не несет новизны – существуют аналогичные обучающие и тестирующие системы, однако внедрение обучающей системы является эффективным. В дальнейшем внедренная система может быть успешно применена внутри компании с возможностью расширения используемой функциональности.

Оглавление

Введение

В настоящее время, в эпоху технического прогресса и стремительного развития информационных систем, остро встают вопросы информационной безопасности и защиты информации. Зачастую, наиболее уязвимым звеном в процессе обработки и передачи информации становится именно человек. Это обусловлено тем, что часто сотрудники не знакомы в должной степени с регламентами и требованиями корпоративных стандартов по информационной безопасности.

Наряду с техническими средствами, одним из способов повышения защищенности информационных систем является обучение сотрудников и контроль уровня их знаний в области информационной безопасности.

Задача данной работы – повышение защищенности информационных систем компании посредством обучения сотрудников требованиям и регламентам информационной безопасности. Известно, что для крупных компаний очень важно грамотно подходить к работе с конфиденциальной информацией клиентов, поэтому обучение должно быть систематическим и направленным на поддержание высокого уровня знаний информационной безопасности.

Актуальность рассматриваемой темы очевидна – непредумышленные нарушения правил информационной безопасности, установленных стандартами компании, могут принести большие убытки и негативно сказаться не только на имидже компании, но и на состоянии ее клиентов, что также может привести к убыткам.

Целью работы является разработка проекта внедрения системы корпоративного обучения, направленного на автоматизацию процесса изучения стандартов безопасности компании Deutsche Telekom и проверки полученных знаний на основе использования тестирования.

Объектом исследования является процесс обучения сотрудников компании Deutsche Telekom.

Предметом исследования является алгоритм внедрения информационной системы для обучения сотрудников и проверки их знаний.

Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать процесс изучения стандартов информационной безопасности сотрудниками компании Deutsche Telekom;
- провести концептуальное моделирование предметной области;
- провести логическое и физическое моделирование предметной области;
- проанализировать существующие разработки и выбрать оптимальное решение для внедрения;
- спроектировать и реализовать серверную инфраструктуру для внедрения
- внедрить систему и оценить экономический эффект.

Структурно работа состоит из трех глав. В первой главе приведен анализ предметной области «информационная безопасность» на примере компании Deutsche Telekom. Здесь же рассмотрены существующие системы обучения, проведено сравнение и выбор.

Во второй главе описан процесс внедрения обучающей системы. Также, в рамках данной главы приводится контрольный пример, демонстрирующий работу внедренной системы.

Третья глава содержит оценку и обоснование экономической эффективности проекта, подтверждая актуальность его внедрения.

Глава 1 Анализ процесса изучения стандартов информационной безопасности сотрудниками Deutsche Telekom

1.1 Технико-экономическая характеристика компании Deutsche Telekom

Компания Deutsche Telekom является крупнейшим провайдером телекоммуникационных услуг на территории Германии. Основными клиентами компании являются контрактные абоненты, однако, есть и услуги, реализуемые в виде предоплаченных карт “Xtra”. Полный спектр предоставляемых услуг очень широк: начиная от консалтинга, проектирования, разработки, внедрения и интеграции, и заканчивая управлением жизненным циклом приложений и хостингом. Стоит отметить, что цены предоставляемых телекоммуникационных услуг являются одними из самых высоких на территории Германии.

В России Deutsche Telekom существует более 23 лет, имея три офиса: в Санкт-Петербурге, Москве и Воронеже. В данный момент интересы всех подразделений компании на территории России и стран СНГ представляет компания ООО «Т-Системс РУС», зарегистрированная в 2014 году.

Данная компания ведёт деятельность по разработке программного обеспечения как для внутренних проектов Deutsche Telekom, так и для внешних заказчиков, например, T-Mobile, Daimler, BMW, Airbus и других.

Работа с такими крупными заказчиками и проектами подразумевает интенсивный документооборот. На каждой из стадий разработки и внедрения проектов используется большой объём документации, в том числе конфиденциальной. В этих условиях крайне важным является вопрос предотвращения инцидентов информационной безопасности.

За годы своей деятельности компания Deutsche Telekom зарекомендовала себя как надежный поставщик интегрированных решений, предназначенных для проектирования корпоративных сетей и центров обработки данных с

высокой степенью защиты, а также уникальной облачной экосистемы, в состав которой входят стандартные платформы и глобальные партнерства.

Важно отметить, что большинство из клиентов компании являются организациями, работающими под юрисдикцией стран Евросоюза и США, и работа с их данными строго регламентирована требованиями данных стран. Кроме того, некоторые из них являются правительственными организациями, например, Министерство обороны Германии, что обуславливает ещё более строгие требования к защите информации.

Таким образом, вопрос безопасности и степени защиты является критичным не только для предоставляемых услуг, но и для внутренней деятельности компании.

Текущая схема организации системы безопасности компании представление на рисунке 1.1.

Рисунок 1.1 - Общая схема системы защиты Deutsche Telekom

Основной стандарт, используемый в компании – ISO/IEC 27001:2013 «Информационная безопасность».

Главной задачей отдела защиты информации является управление инцидентами информационной безопасности (ИБ). Под инцидентом ИБ понимается возникновение одного или нескольких неожиданных событий ИБ, которые с большой вероятностью приводят к компрометации бизнес-информации, а также создают угрозы ИБ в целом.

Управление инцидентами представляет собой деятельность по своевременному обнаружению инцидентов ИБ, адекватному и оперативному реагированию на них, направленная на минимизацию и (или) ликвидацию негативных последствий от инцидентов ИБ для компании и ее клиентов [21].

Инцидентами ИБ являются любые инциденты, имеющие следующие признаки:

- физический доступ посторонних лиц в здания и помещения компании;
- сбои в работе системы контроля физического доступа (система контроля доступа, замки дверей, система видеонаблюдения);
- разглашение персональных данных компании и сотрудников;
- неавторизованный доступ к информации;
- кража оборудования и других основных средств компании;
- сбои и отказы в работе средств вычислительной техники, телекоммуникационного оборудования;
- несанкционированное изменение параметров и настроек средств вычислительной техники, телекоммуникационного оборудования, сетей передачи данных и телефонной связи;
- несанкционированный вынос за пределы компании средств вычислительной техники и носителей информации;
- обнаружение аномальной сетевой активности;

- необоснованное отключение/перезагрузка средств вычислительной техники, сетевого и другого оборудования;
- сбои в работе средств защиты информации (антивирусы, сетевые экраны);
- разглашение аутентификационных данных, в том числе паролей, используемых для доступа к ИТ-ресурсам и оборудованию компании;
- обнаружение нетипичных запросов на уровне сетевых приложений и сервисов [6].

Основными источниками инцидентов ИБ являются:

- программные и технические средства:
  - системные журналы операционных систем;
  - системные журналы систем управления базами данных;
  - регистрационные журналы прикладного программного обеспечения;
  - регистрационные журналы активного сетевого оборудования;
  - журналы применяемых средств защиты информации;
  - информация специализированных устройств контроля физического доступа;
- сотрудники компании, обнаружившие инцидент ИБ;
- клиенты и партнеры компании.

Обработка инцидентов информационной безопасности происходит по следующему алгоритму:

- обнаружение и регистрация инцидентов ИБ;
- категорирование событий, сбор дополнительной информации и выявление инцидентов ИБ;
- оповещение группы реагирования на инцидент, вторичная оценка инцидента ИБ и его приоритизация;
- реагирование на инцидент и устранение всех последствий, вызванных инцидентом;

- расследование инцидента, определение причин его возникновения и предотвращение подобных инцидентов в будущем.

Схема работы с инцидентами информационной безопасности представлена на рисунке 1.2

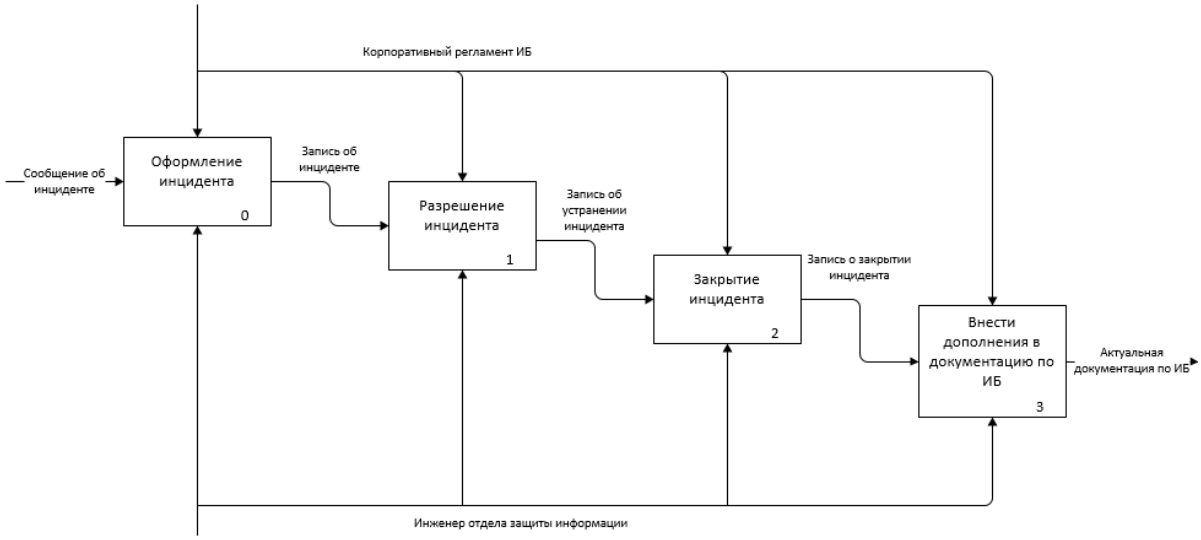

Рисунок 1.2 – Схема работы с инцидентами ИБ

Стоит отметить, что уровень знания требований и регламентов информационной безопасности у сотрудников различается. Некоторые из сотрудников могут иметь пробелы в знаниях, что влечёт за собой риски возникновения инцидентов информационной безопасности.

Также, вновь принятые сотрудники получают доступ к конфиденциальной информации компании сразу после регистрации их в информационных системах, без проверки уровня их знаний в области информационной безопасности.

Для решения этих проблем и повышения общего уровня знаний, рекомендуется использовать систему корпоративного обучения. Это позволит как проводить инструктаж и обучение сотрудников, так и предоставлять им доступ к конфиденциальной информации после успешно пройденного тестирования.

1.2 Сущность задачи повышения информационной безопасности путём использования системы корпоративного обучения

Одним из слабых мест компании Deutsche Telekom является первичное обучение сотрудников основам информационной безопасности, что подтверждается случаями нарушения установленных стандартов.

Существующая схема системы безопасности внутри компании не предусматривает тестирования сотрудников. Поэтому для сбора статистических данных, отображающих динамику развития сотрудников, необходимо хранить их результаты прохождения тестирования на протяжении всего периода работы.

Эти показатели позволят анализировать общий уровень знаний сотрудников и динамику их изменения с течением времени.

Задачей данной выпускной квалификационной работы является решение проблемы недостаточного знания требований и регламентов информационной безопасности сотрудниками компании.

Одним из способов решения данной проблемы является использование информационной системы для инструктажей и обучения сотрудников общим и корпоративным стандартам информационной безопасности, что позволяет сократить возникновение числа инцидентов ИБ внутри компании.

Важно понимать, что именно человеческий фактор является ключевым в процессе обеспечения требуемого уровня безопасности. Именно по этой причине все сотрудники компании Deutsche Telekom должны проходить обязательное обучение политике безопасности для досконального понимания возможных угроз информационной безопасности [22].

Основные цели обучения сотрудников в области информационной безопасности внутри компании:

- понимание политики ИБ как внутри компании, так и по отношению к ее клиентам;
- знание требований ИБ в рамках компании;

- понимание собственных обязанностей и функций, связанных с обеспечением безопасности;
- обладание знаниями в области управленческого, операционного и технического контроля над усилением защиты интеллектуальной собственности внутри их зон ответственности.

В результате проведения данных тренингов общий уровень безопасности в компании должен увеличиться.

Таким образом, в рамках данного параграфа приводятся данные об общей деятельности компании Deutsche Telekom, характеризуется структура системы безопасности, действующей в компании, её недостатки, а также описывается сущность задачи внедрения системы обучения сотрудников.

1.3 Концептуальное моделирование процесса изучения стандартов информационной безопасности сотрудниками Deutsche Telekom

В настоящее время в большинстве отделов компании задача первичного обучения сотрудников вопросам информационной безопасности уходит на второй план в силу того, что человеку даются узконаправленные тренинги, необходимые для его непосредственной профессиональной деятельности.

Требование соблюдения корпоративных регламентов ИБ является одним из пунктов трудового договора, который сотрудники подписывают в процессе приема на работу.

Первичное ознакомление с требованиями информационной безопасности происходит после выхода сотрудника на работу.

В данной процедуре имеется недостаток – процесс ознакомления происходит через доступ к внутренним статичным веб ресурсам, и нет технической возможности проконтролировать прошёл ли сотрудник инструктаж, и насколько он усвоил прочитанный материал. Текущая схема трудоустройства новых сотрудников представлена на рисунке 1.3.

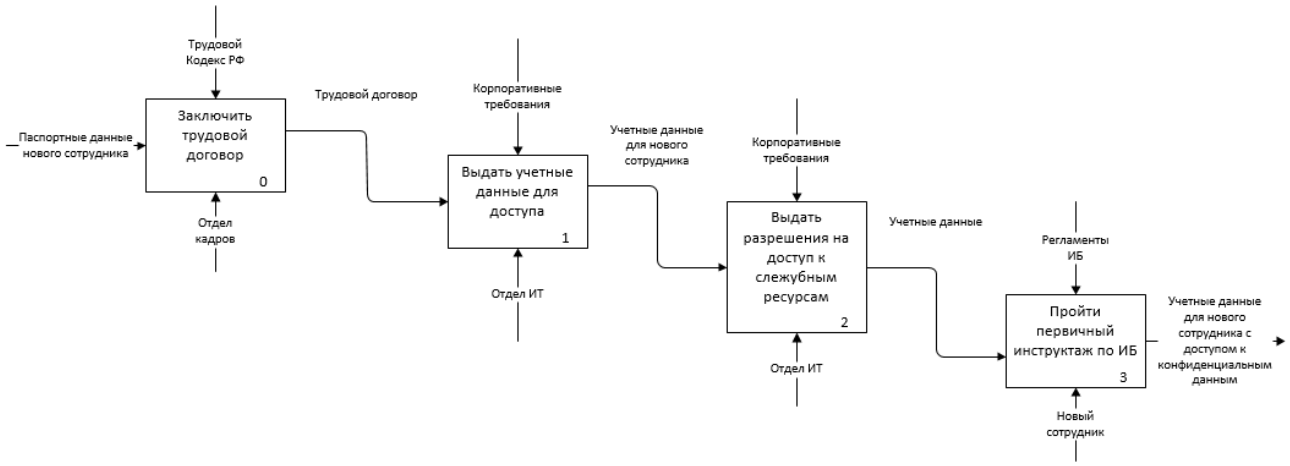

Рисунок 1.3 – Текущая схема трудоустройства новых сотрудников

Как видно из представленной схемы, при текущей организации процессов новый сотрудник получает доступ ко внутренним ресурсам компании ещё до прохождения первичного инструктажа и без контроля полученных знаний. Это потенциально повышает опасность возникновения инцидентов информационной безопасности.

Путём внедрения обучающего комплекса, становится возможным решить проблему недостаточного знания сотрудниками компании требований информационной безопасности. Также, это позволит изменить процесс регистрации в ИТ системах предприятия вновь принятых сотрудников таким образом, чтобы разрешения на доступ к конфиденциальным ресурсам компании выдавались только после прохождения инструктажа на учебной платформе с последующей успешной сдачей тестирования.

К внедряемому решению предъявляются следующие требования:

- наличие возможности динамически создавать и редактировать обучающие курсы;
- наличие возможности создавать тесты в рамках учебных курсов;
- наличие возможности использования в тестах различных вариантов вопросов: с одним выбором, с множественным выбором, с вводом текста через поле ввода;

- наличие возможности устанавливать оценки в баллах за каждый из вопросов;
- наличие возможности устанавливать проходной балл для успешного прохождения теста;
- наличие возможности просматривать результаты тестирований сотрудников администратором системы.

Тогда процесс приёма новых сотрудников будет выглядеть согласно схеме на рисунке 1.5.

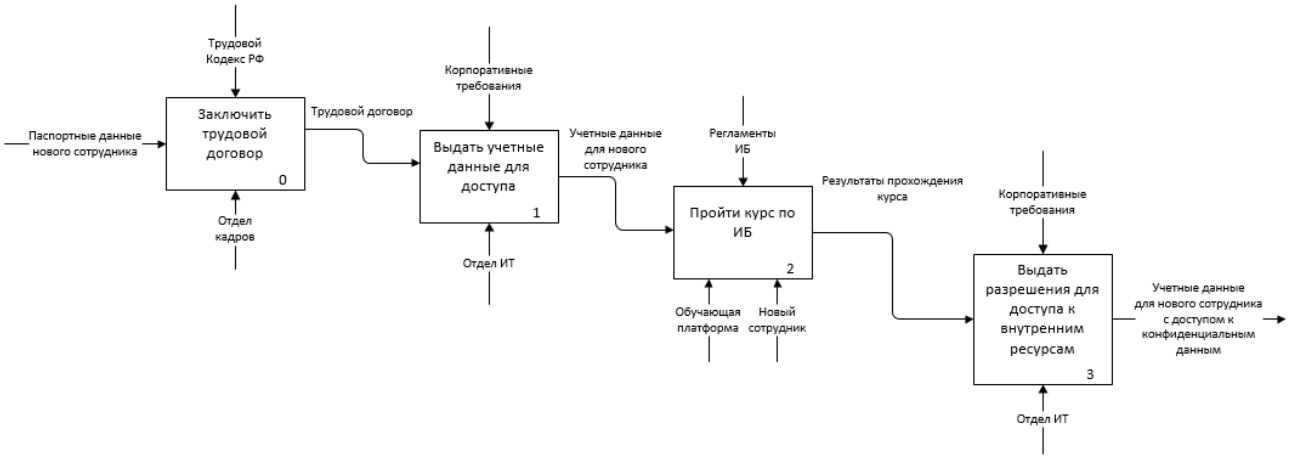

Рисунок 1.4 – Схема трудоустройства новых сотрудников после внедрения обучающей системы

Таким образом, путём внедрения обучающего решения становится возможным снизить риски информационной безопасности, так как новые сотрудники не получают прав для доступа к служебным ресурсам до прохождения курса по ИБ.

1.4 Бизнес-цель и назначение корпоративной системы обучения

Система корпоративного обучения – десктоп или веб приложение, используемое для планирования, реализации и оценки процесса обучения сотрудников. Обычно, такая система предоставляет средства для создания и доставки теоретического и практического материала, наблюдения за изучением и оценки их успеваемости.

Бизнес-целью внедрения системы корпоративного обучения является устранение опасности возникновения инцидентов информационной безопасности, вызванных недостаточными знаниями сотрудников в области информационной безопасности.

Назначение реализации внедрения системы обучения:

- автоматизация процессов инструктажей и обучения сотрудников;
- автоматизация процесса проверки знаний сотрудников, полученных в процессе обучения;
- снижение рисков возникновения инцидентов информационной безопасности.

Повышение общего уровня компетенции сотрудников в сфере информационной безопасности приведёт к общему росту защищенности информационных систем компании.

Процесс решения поставленной задачи разбивается на ряд подзадач:

- анализ существующих на рынке решений
- выбор решения для внедрения
- сбор данных для обучения;
- разработка теоретической части программы обучения;
- разработка практической части программы обучения.

Таким образом, для решения поставленной задачи необходимо:

- проанализировать имеющиеся разработки
- выбрать оптимальное решение для внедрения
- изучить общий стандарт безопасности;
- изучить корпоративный стандарт безопасности;
- составить практическую часть для проверки знаний сотрудников в виде теста.

Поскольку, согласно определению, обучающая система предоставляет средства для создания и наполнения учебных курсов, следовательно, в

дальнейшем она может применяться для обучения также и другим дисциплинам.

1.5 Анализ существующих разработок и обоснование выбора технологии проектирования

1.5.1 Определение критериев анализа существующих разработок

Рынок современных информационных технологий предлагает целое множество приложений, направленных на обучение и тестирование.

При рассмотрении этих приложений в рамках поставленной задачи необходимо обращать внимание на три параметра:

- возможности системы;
- стоимость системы;
- технические требования системы.

С точки зрения функциональных возможностей будущая система должна позволять решать следующие задачи:

- поддержка работы с теоретическими материалами: создание курсов, наполнение учебным материалом;
- поддержка работы с практическими материалами: создание тестов в курсах;
- ведение статистики результатов;
- предоставление отчетов.

Проанализировав каждую из платформ обучения по вышеописанным пунктам, можно определить оптимальную для внедрения в организации.

1.5.2 Характеристика существующих систем корпоративного обучения

В первую очередь, требуется проанализировать наличие на рынке готовых систем обучения информационной безопасности. В силу того, что данное направление обучения довольно узкоспециализировано, а также может не включать в себя корпоративные регламенты компании, было принято

решение использовать обучающую платформу, с возможностью создания и наполнения курсов.

В настоящее время одной из наиболее популярных платформ для реализации систем корпоративного обучения, применяемых в коммерческих компаниях, является Moodle.

Moodle представляет собой среду дистанционного обучения, в которой можно создавать и хранить любые учебные материалы, а также задавать их последовательность обучения для сотрудников.

В силу того, что Moodle является дистанционной системой, ее могут использовать сотрудники любых филиалов компании через веб интерфейс, без установки каких-либо приложений [18].

Имеющийся электронный формат позволяет оперировать не только текстовыми учебными материалами, но и интерактивными ресурсами, начиная от web-статей и заканчивая видеороликами.

Еще одним преимуществом данной системы является возможность ее совместного использования. При этом обучение может происходить как асинхронно, так и в режиме реального времени, когда сразу несколько сотрудников будут изучать одни и те же материалы.

Результаты обучения каждого сотрудника хранятся в специальном портфолио, содержащем сведения о сданных тестах, оценках и комментариях преподавателей.

Стоит отметить, что система распространяется в открытом коде и является бесплатным продуктом. Кроме того, она содержит специальные средства разработки дистанционных курсов, за счет которых снижается стоимость решения проблем совместимости с другими курсами. Также существует возможность разработки дополнительных модулей (плагинов) для данной системы [19].

Таким образом, Moodle является очень гибкой платформой, способной удовлетворить самые строгие требования.

Еще одной популярной платформой является WebTutor – система дистанционного обучения, развития и подбора персонала от компании WebSoft.

Данная система предполагает использование двух ролей:

- администраторы – пользователи, способные управлять всеми процессами существующей системы;
- обучаемые – непосредственные пользователи системы.

Система WebTutor состоит из нескольких модулей, основными из которых являются:

- персонал – модуль, отвечающий за ведение списков пользователей и формирование их в специальные группы для обучения;
- дистанционное обучение – модуль, формирующий электронные курсы и отвечающий за реализацию доступа к этим курсам;
- тестирование – модуль редактора и прохождения тестов;
- управление знаниями – построение карты и профилей знаний, настройка связей между информационными материалами и т.п.;
- библиотека – модуль теоретических данных;
- подбор персонала - модуль предназначен для организации подбора персонала при помощи рекрутинговых агентств и специализированных сайтов.

Однако, WebTutor является платным приложением, и, кроме того, значительно уступает Moodle в функциональности и гибкости. Таким образом, было принято решение внедрить Moodle для решения поставленных задач.

Таким образом, в данном параграфе были рассмотрены две популярные платформы дистанционного обучения, описаны их основные возможности. Исходя из полученных данных, становится возможным выбрать систему, максимально удовлетворяющую требованиям заказчика и разработать проект по внедрению данной системы.

Выводы по главе 1

В данной главе работы приведен анализ предметной области. Описана характеристика компании Deutsche Telekom, являющейся крупнейшим провайдером телекоммуникационных услуг на территории Германии.

Работа над ВКР ведется в отделе защиты информации, главной задачей которого является управление инцидентами информационной безопасности.

В связи с тем, что деятельность компании предъявляет обуславливает высокие требования к уровню информационной безопасности, в рамках ВКР была поставлена задача, заключающаяся в повышении информационной безопасности компании путём обучения сотрудников компании требованиям информационной безопасности. Для этого необходимо внедрить систему корпоративного обучения с возможностью контроля полученных знаний, проведения периодических проверок и обновления учебных курсов.

Здесь же проводится концептуальное моделирование предметной области – описывается существующий подход и обосновывается необходимость внедрения системы обучения.

Также, в данной главе описаны существующие платформы Moodle и WebTutor. В результате было принято решение реализации корпоративной системы обучения на базе Moodle, так как данная платформа полностью удовлетворяет требованиям компании и является бесплатной.

Глава 2 Разработка проектных решений по обучению сотрудников

2.1 Классы и формализация пользователей программного проекта

Важным этапом разработки проекта внедрения системы является этап определения и формализации классов пользователей. Определяющим фактором в этом процессе являются особенности заказчика, потенциальных пользователей и заинтересованных лиц.

В корпоративной обучающей системе Deutsche Telekom предполагается наличие двух ролей:

- пользователь;
- администратор.

Бизнес-роль пользователя предполагает взаимодействие с учебной системой с целью прохождения учебных курсов и дальнейшей сдачей тестов по пройденным курсам. Для выполнения данной работы пользователю требуется получить учётные данные (логин и пароль) от администратора учебной системы. Работа считается выполненной после успешного прохождения тестирования, когда пользователь получил за тест количество баллов, превышающее проходное значение. Функциональная схема пользователя представлена на рисунке 2.1.

Бизнес-роль администратора предполагает взаимодействие с учебной системой со следующими целями:

- регистрация нового пользователя в системе;
- создание и наполнение учебных курсов, в том числе тестами;
- просмотр результатов прохождения учебных курсов;
- подтверждение выдачи разрешений на доступ к конфиденциальной информации для вновь принятых сотрудников по результатам прохождения теста.

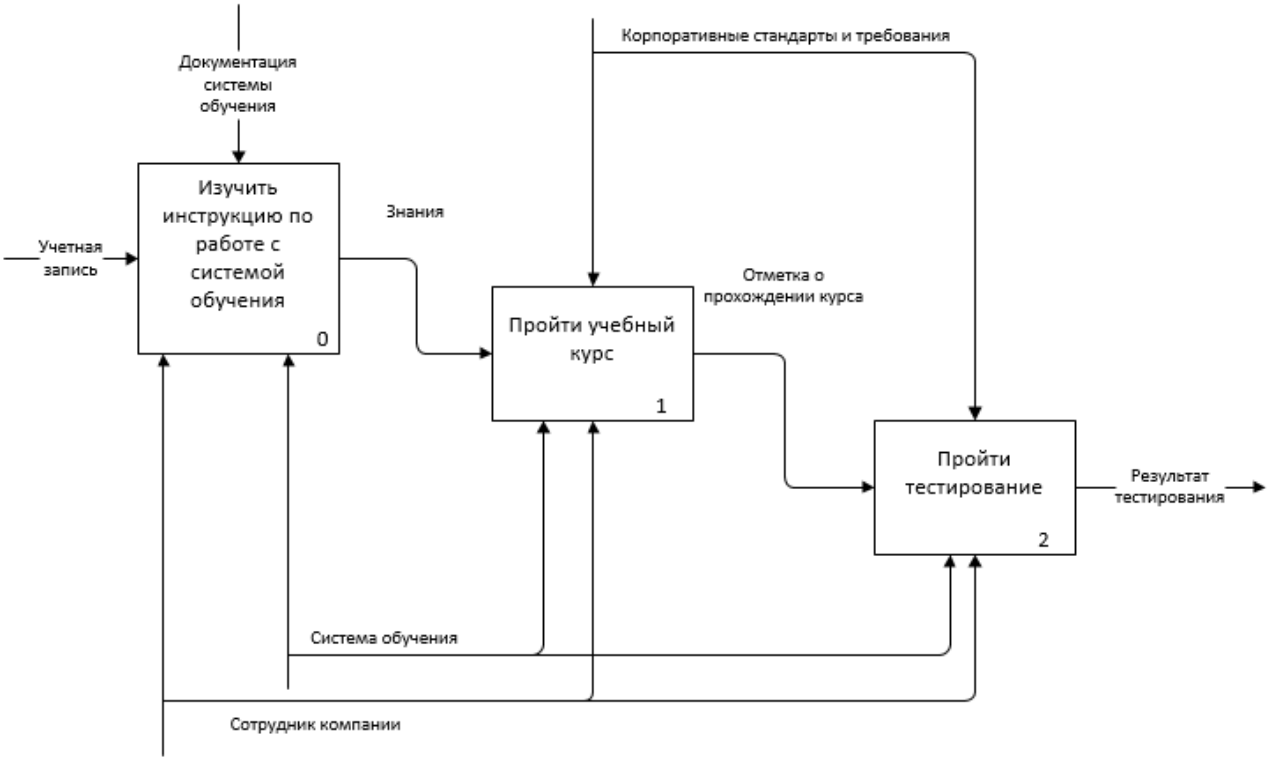

Рисунок 2.1 - Функциональная схема для пользователя

В первую очередь, для выполнения данных задач, администратору требуется получить учётные данные (логин и пароль) от учётной записи, имеющей роль «администратор» в обучающей системе. Первоначальная запись администратора создаётся при разворачивании учебной системы, в дальнейшем, используя эту запись, можно создать неограниченное количество дополнительных учётных записей администраторов. Для создания и наполнения учебных курсов, администратору требуется получить теоретический материал от Отдела защиты информации, а также список вопросов и ответов для теста с критериями оценки: количество баллов за каждый из вопросов и минимальный балл для успешного прохождения теста.

Функциональная схема администратора представлена на рисунке 2.2.

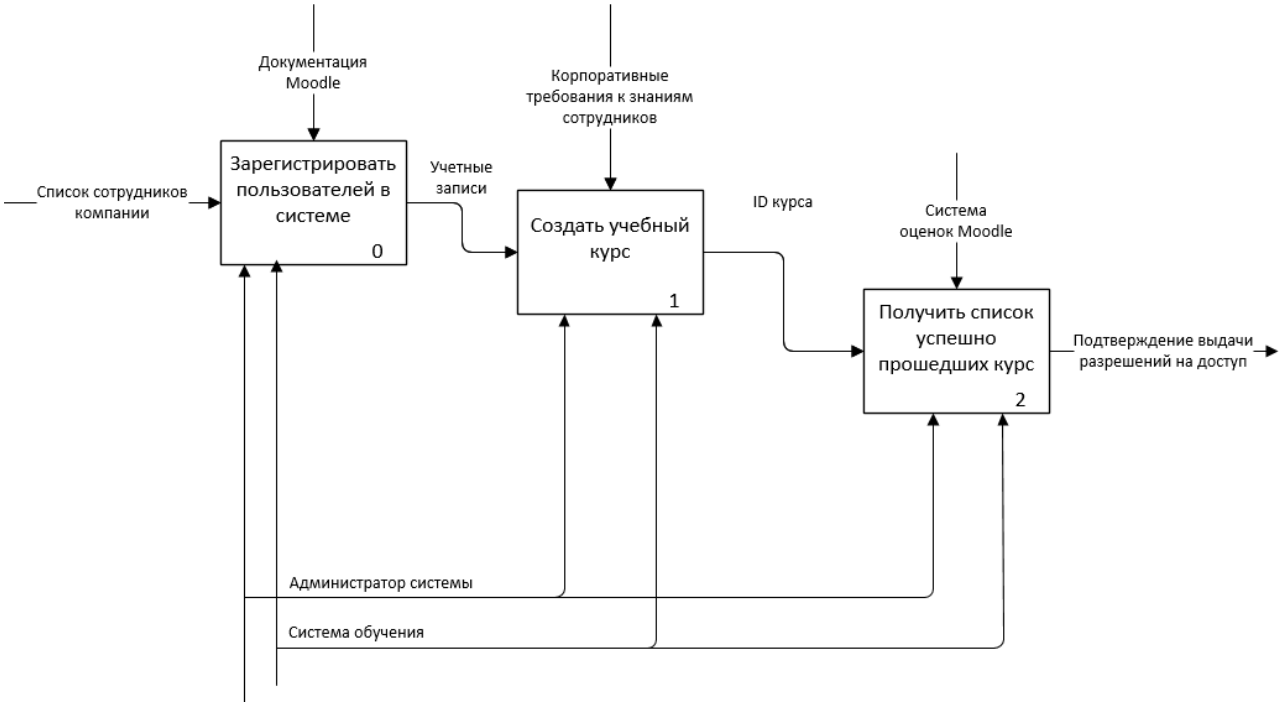

Рисунок 2.2 - Функциональная схема для администратора

Таким образом, определив роли пользователей системы и функциональные схемы для них, можно перейти к описанию функциональных требований проекта.

2.2 Описание функциональных требований проекта

Для разработки проектного решения требуется охарактеризовать требования и описать методики их выявления. При работе с заказчиком Deutsche Telekom будут использованы методы: изучение существующей документации и интервью. Метод изучения существующей документации может быть использован при наличии у заказчика регламентов и описания процессов в требуемой области, однако этого недостаточно, так как имеющиеся документы не описывают процесса обучения сотрудников и регламента предоставления доступа к конфиденциальной информации строго после тестирования. Для определения требований к новой функциональности, дополнительно используется метод интервью с руководителем отдела по защите информации. Для моделирования бизнес-логики используется нотация

BPMN, так как это распространённая и простая для восприятия нотация, позволяющая реализовать концепцию непосредственного исполнения бизнес-процесса. Модель бизнес-процесса приёма нового сотрудника и предоставления ему доступа к конфиденциальным данным компании представлена на рисунке 2.3.

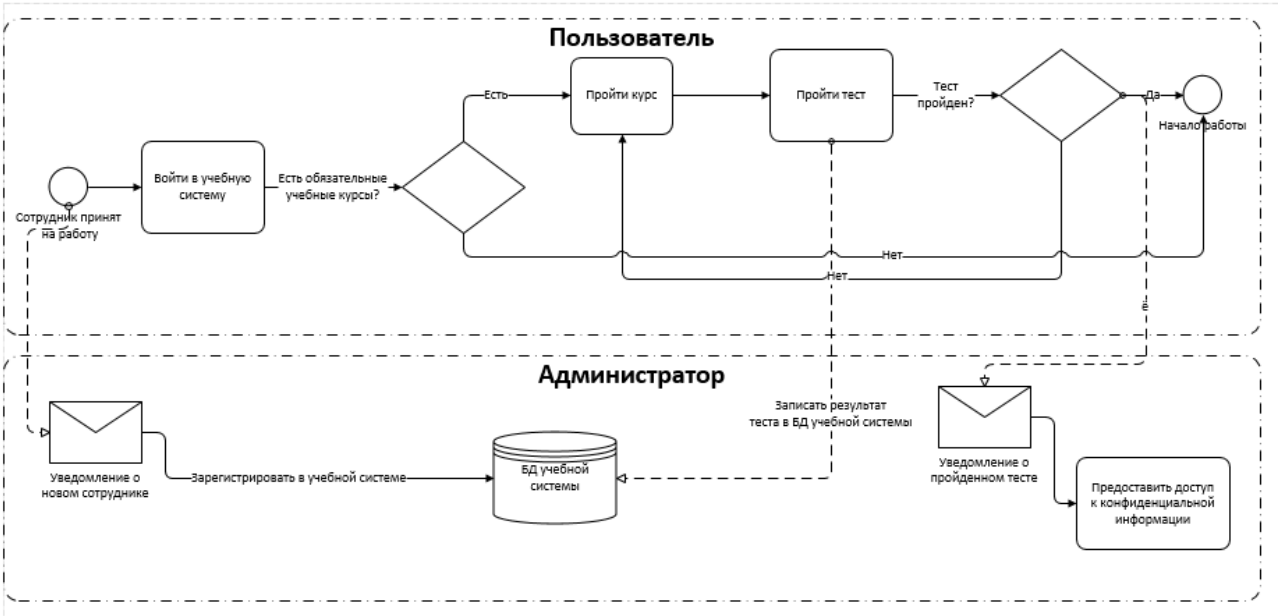

Рисунок 2.3 – Процесс приёма нового сотрудника и предоставление ему доступа к конфиденциальным данным

С точки зрения функциональных требований, выделяются следующие блоки:

- необходимая функциональность:
  - возможность регистрации пользователей;
  - возможность создания учебных курсов с теоретическим материалом, в том числе в виде видео и графики;
  - возможность создания тестов в рамках учебных курсов, с наполнением вопросами, установкой количества баллов за каждый из вопросов и установкой минимального количества баллов для успешного прохождения теста.
- желательная функциональность:

- возможность информирования администраторов о прохождении тестов;
- возможность интеграции с внешним LDAP сервером для аутентификации пользователей.

В качестве нефункциональных требований выступают следующие:

- отклик на каждую операцию не более 100 мс при установке на виртуальную машину с 4 ядрами ЦПУ и 16 Гб ОЗУ и сетевым интерфейсом с пропускной способностью 1 Гбит;
- поддержка установки на виртуальную машину под управлением ОС Linux CentOS 7;
- наличие документации по установке и поддержке, выполнению типовых операций.

При условии выполнения данных требований, система обучения может быть внедрена для нужд заказчика.

2.3 Логическое моделирование процесса изучения стандартов информационной безопасности сотрудниками Deutsche Telekom

Основная задача построения логической модели - создание графического представления логической структуры исследуемой предметной области [3].

Логическая модель характеризует сущности и их взаимоотношения. В качестве сущностей используются объекты, являющиеся предметом деятельности в рассматриваемой области, и субъекты, реализующие деятельность. Свойства объектов и субъектов реального мира описываются с помощью атрибутов.

Установленные взаимоотношения между сущностями отображаются с помощью связей. Чаще всего связи определяют либо зависимости между сущностями, либо влияние одной сущности на другую.

Сущности рассматриваемой предметной области:

- сотрудники;

- учебные предметы;
- тесты по предметам.

Сущность «сотрудник» представляет собой совокупность данных уникального табельного номера и паспортных данных (фамилии, имени, отчества).

Сущность «учебный предмет» представляет собой курс в системе Moodle, с которым ассоциированы теоретические материалы и опционально один или более тестов.

Сущность «тест» представляет собой совокупность множества вопросов с различными вариантами ответа:

- один ответ;
- несколько ответов;
- ответ через поле ввода (например, число).

Для хранения баллов, полученных каждым сотрудником по результатам теста, используется база данных Moodle.

Полученная логическая модель системы корпоративного обучения представлена на рисунке 2.4.

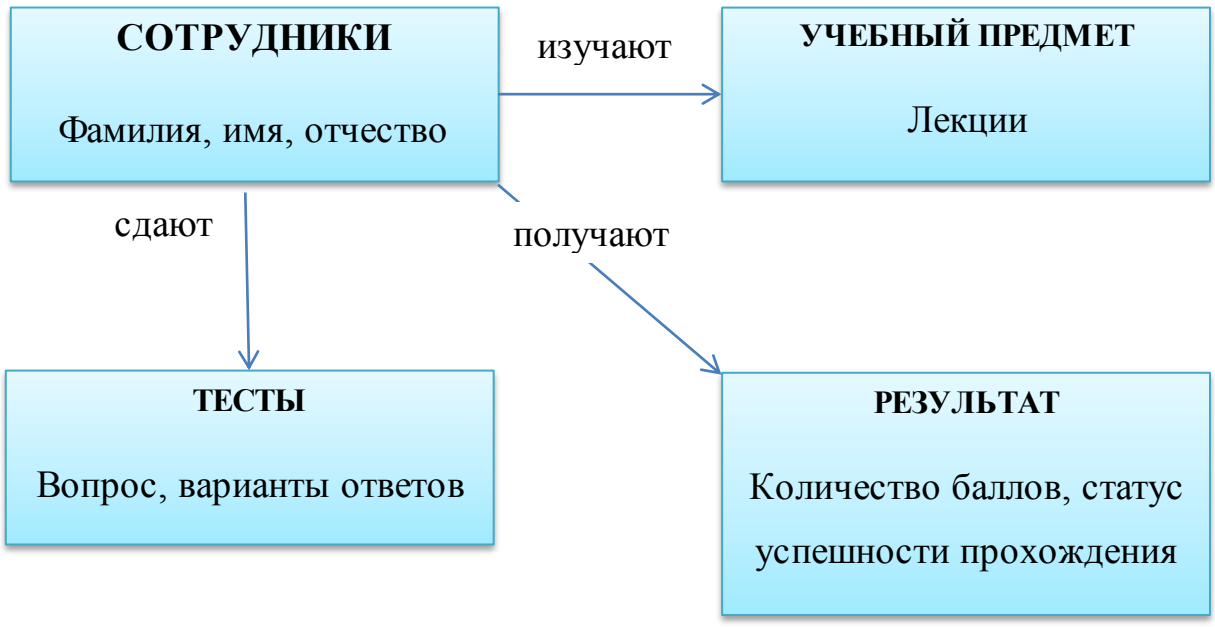

Рисунок 2.4 - Логическая модель системы проверки знаний

Таким образом, в рамках данного параграфа описывается логическая модель предметной области – выделены основные сущности, их атрибуты и связи.

2.4 Физическое моделирование системы обучения

Этап физического моделирования служит для обеспечения на экспериментальном уровне проверки реальной работоспособности созданной логической модели и ее адекватности. Задача данного этапа – разработка физической модели, которая представляет собой совокупность структуры, методов и средств редуцированного воплощения системы, предназначенная для проверки в реальных условиях работоспособности будущей системы и адекватности ее моделей [12].

Физическая модель должна обладать свойствами реальной системы. Для ее построения могут быть использованы ЭВМ, периферийные устройства, документы, файлы, БД и т.п.

Свойство редуцированности модели говорит о том, что она является «уменьшенным» отображением реальной системы – содержит только те свойства, которые являются существенными, основными [15].

Для системы обучения необходимо использование клиент-серверной архитектуры. Необходимо наличие возможности использовать в качестве клиента как стационарные компьютеры, так и ноутбуки и мобильные устройства. Данная архитектура максимально эффективна для применения в крупной организации, так как она отказоустойчива и масштабируема. Клиент-серверная архитектура системы обучения приведена на рисунке 2.5.

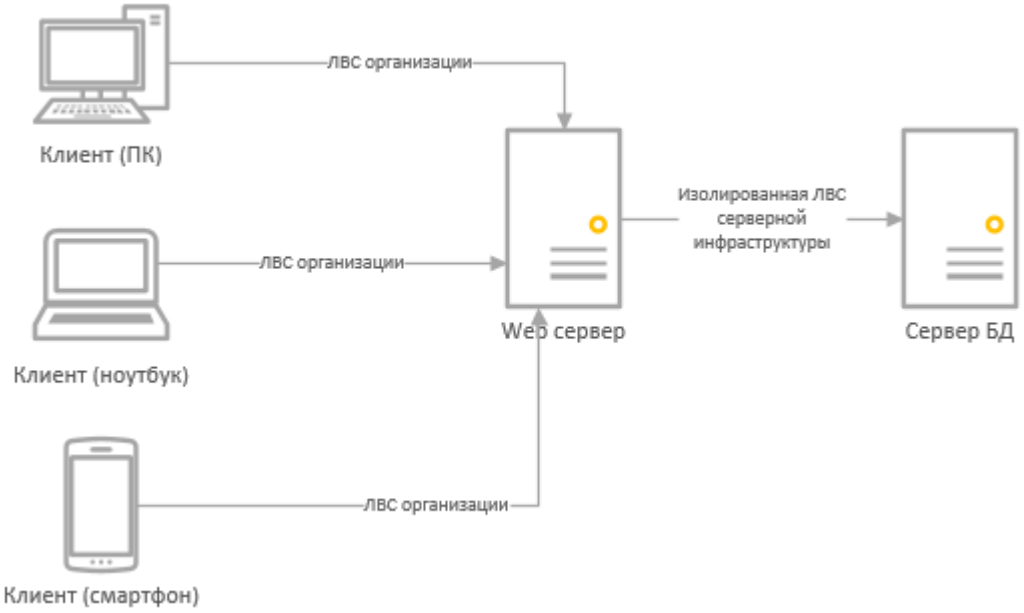

Рисунок 2.5 – Клиент-серверная архитектура системы обучения

Схема используемой базы данных представлен на рисунке 2.6

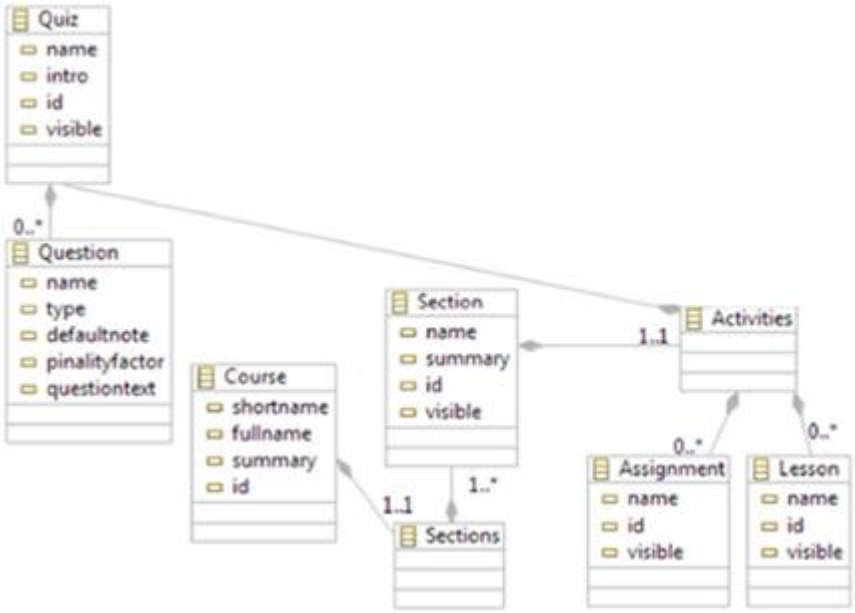

Рисунок 2.6 – Схема БД системы обучения

Система обучения должна поддерживать базу данных PostgreSQL. Для внедрения в Deutsche Telekom был выбран именно PostgreSQL по причине ряда

преимуществ: бесплатность, стабильная работа под высокой нагрузкой, поддержка мультиверсионирования (MVCC), широкие возможности настройки.

2.4.1 Структурная схема проекта обучения сотрудников

Структурная схема проекта обучения сотрудников приведена на рисунке 2.7 [8].

Для использования внедряемой системы необходимы следующие сервисы:

- база данных;
- веб сервер;
- PHP интерпретатор для веб сервера.

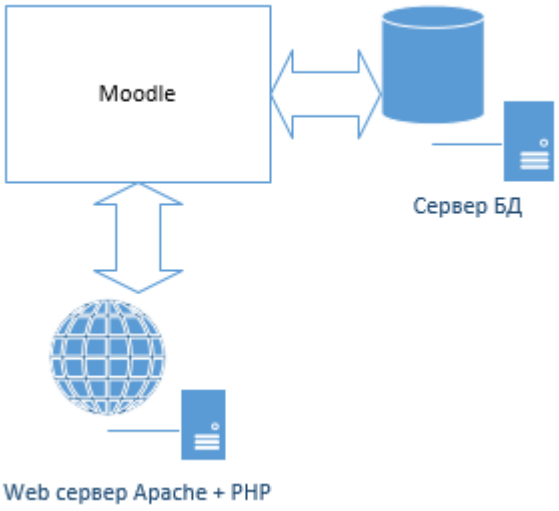

Рисунок 2.7 - Структурная схема

Как видно из представленной схемы, для функционирования Moodle необходимы веб сервер Apache с поддержкой PHP для выполнения программного кода и обеспечения доступа через web интерфейс, и база данных для хранения курсов и результатов их прохождения.

Таким образом, в данном параграфе описывается физическая модель информационной системы и ее функции для различных групп пользователей.

2.5 Технологическое обеспечение задачи обучения сотрудников

Работа с системой пользователя любой роли начинается с процедуры аутентификации через web интерфейс приложения. При неудачной попытке аутентификации пользователю будет предложено повторить ввод или запустить процедуру восстановления пароля посредством отправки сообщения на адрес электронной почты, указанный в профиле пользователя.

После успешной аутентификации пользователю на домашней странице будут отображены доступные для прохождения курсы, также доступны ссылки на профиль пользователя, страницу настроек и календарь, в котором можно посмотреть расписание учебных курсов, имеющих установленные календарные ограничения по прохождению.

В профиле пользователь может редактировать личные данные: имя, фамилию, адрес электронной почты, пароль, а также ряд необязательных полей.

При переходе по ссылке в один из курсов, происходит отображение содержания курса и отметки о прохождении этапов.

Работа с системой осуществляется в событийных и диалоговых режимах. Под диалогом здесь понимается предоставление пользователю нескольких альтернатив и обработка его выбора.

Под событиями понимаются процессы, активизируемые пользователем, а также программные события – получение определенным полем фокуса редактирование или потеря фокуса ввода. На основании этих событий активизируются процедуры проверки корректности введённых данных.

Схематическое представление технологического обеспечения представлено на рисунке 2.8 [12].

Таким образом, в данном параграфе приводится описание технологического обеспечения задачи.

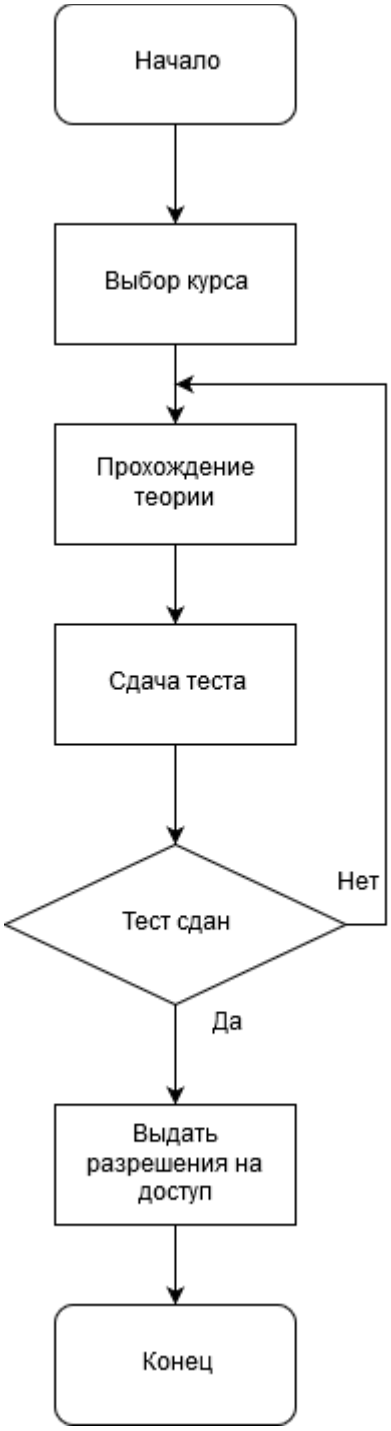

Рисунок 2.8 - Схема сбора, передачи, обработки и выдачи информации

2.6 Контрольный пример реализации проекта и его описание

Запуск приложения происходит одновременно с запуском веб сервера. После того, как приложение полностью загружено, оно становится доступным через веб интерфейс в соответствии с настройками веб сервера (IP адрес и порт). Интерфейс аутентификации пользователя отображен на рисунке 2.9.

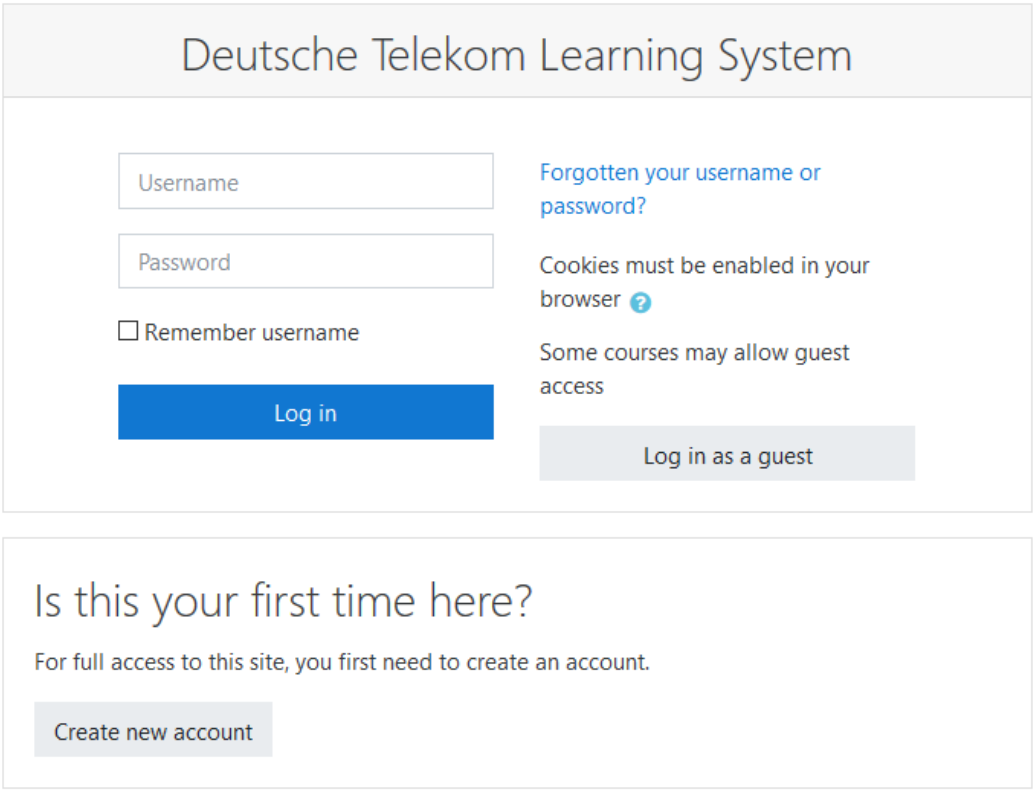

Рисунок 2.9 - Интерфейс аутентификации пользователя

После прохождения аутентификации, пользователю открывается его домашняя страница в Moodle со списком доступных курсов. Интерфейс изображён на рисунке 2.10.

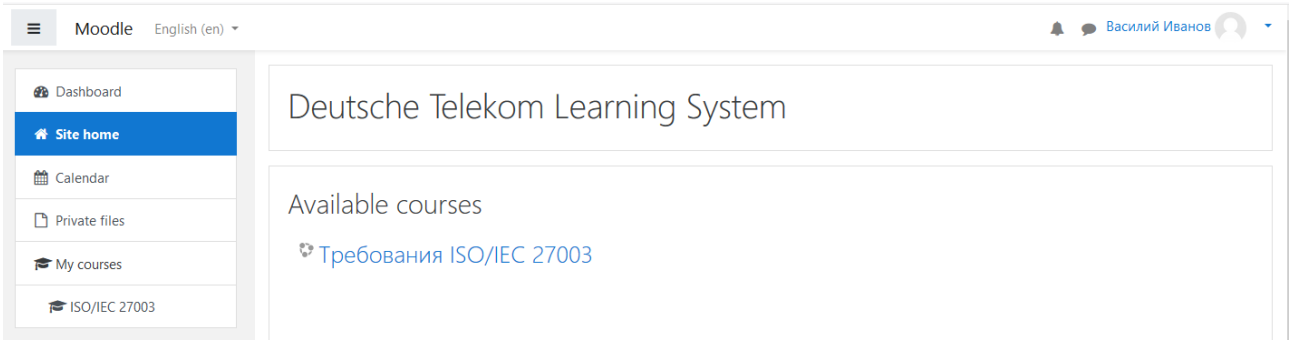

Рисунок 2.10 – Домашняя страница пользователя в Moodle

При переходе по ссылке страницы курса, откроется программа курса, которая может включать в себя теоретический и практический материал, а также отметки о выполнении. Интерфейс представлен на рисунке 2.11.

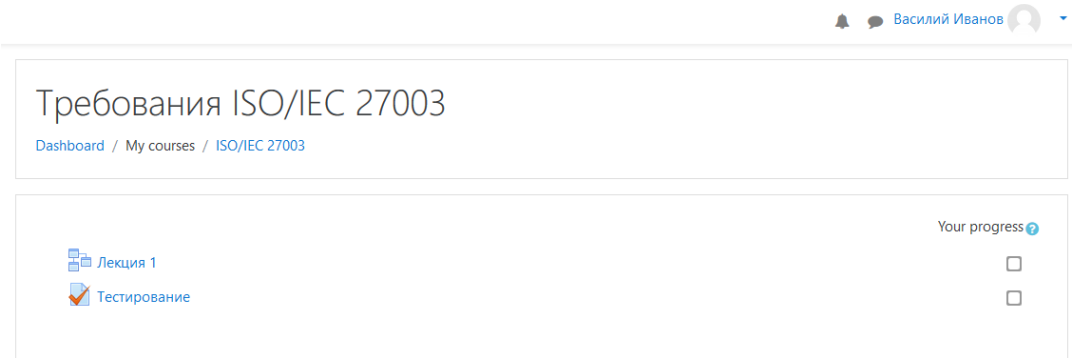

Рисунок 2.11 – Содержание курса

Курс по требованиям стандарта ISO/IEC 27003 состоит из одной лекции и одного теста. При переходе по ссылке лекции, открывается содержание лекции с возможность навигации по разделам, см. рисунок 2.12.

Рисунок 2.12 – Навигация по разделам лекции

По окончанию прохождения теоретической части, пользователь должен пройти практическую часть по данной теме. Практическая часть представлена в виде теста. Вопросы в тесте могут варьироваться: иметь один правильный ответ, несколько правильных ответов (мультивыбор), или же требовать введения правильного ответа в поле ввода (например, при каких-либо расчётах). Внешний вид теста показан на рисунках 2.13-2.14.

Рисунок 2.13 – Вопросы с одним вариантом выбора

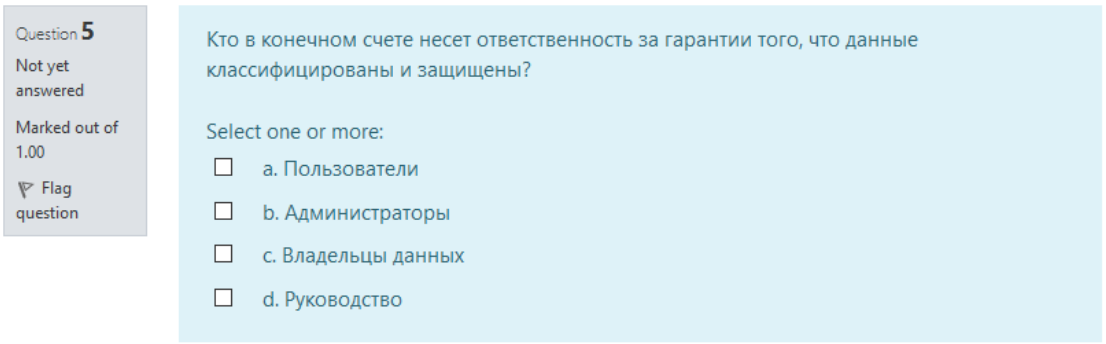

Рисунок 2.14 – Вопрос с несколькими вариантами выбора

После прохождения тестирования, сотруднику отображаются итоговые результаты. Пример показан на рисунке 2.15.

Рисунок 2.15 – Результаты тестирования

Администратор системы взаимодействует с ней также через веб интерфейс. После аутентификации пользователя с ролью «администратор» становятся доступны пункты меню, связанные с администрированием системы. Таким образом можно регистрировать пользователей, создавать курсы, наполнять их содержимым и контролировать их прохождение пользователями. Интерфейса администратора показан на рисунках 2.16-2.18.

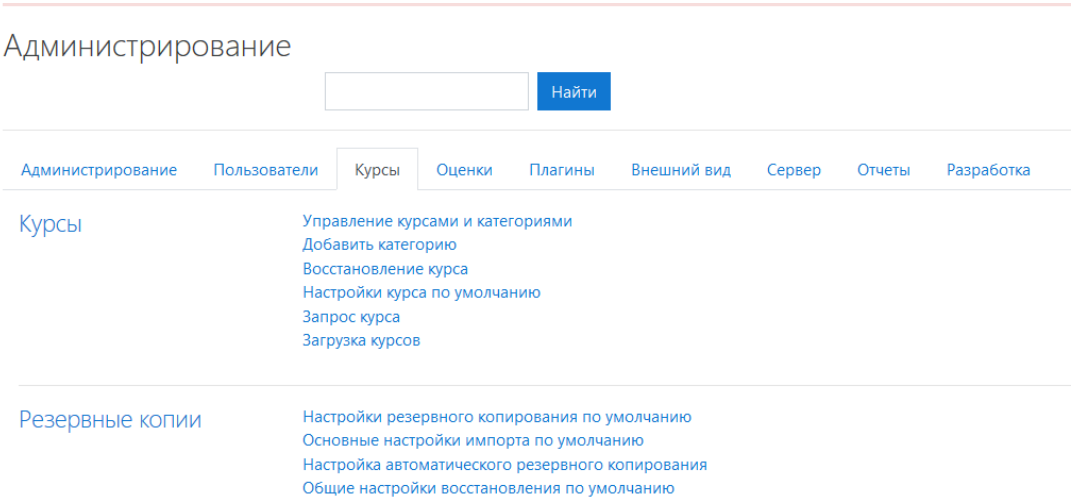

Рисунок 2.16 – Интерфейс администрирования

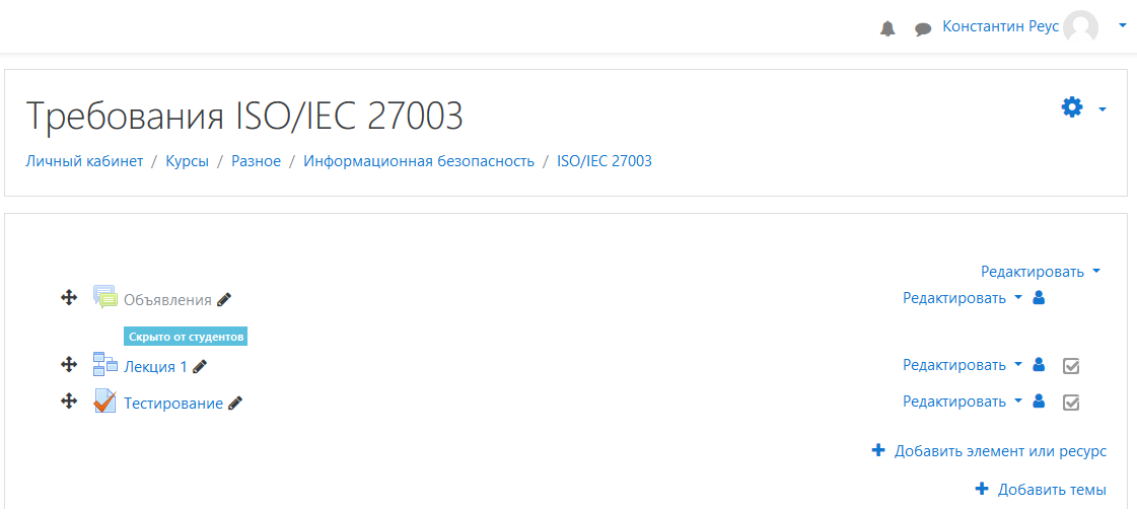

Рисунок 2.17 – Редактирование курса

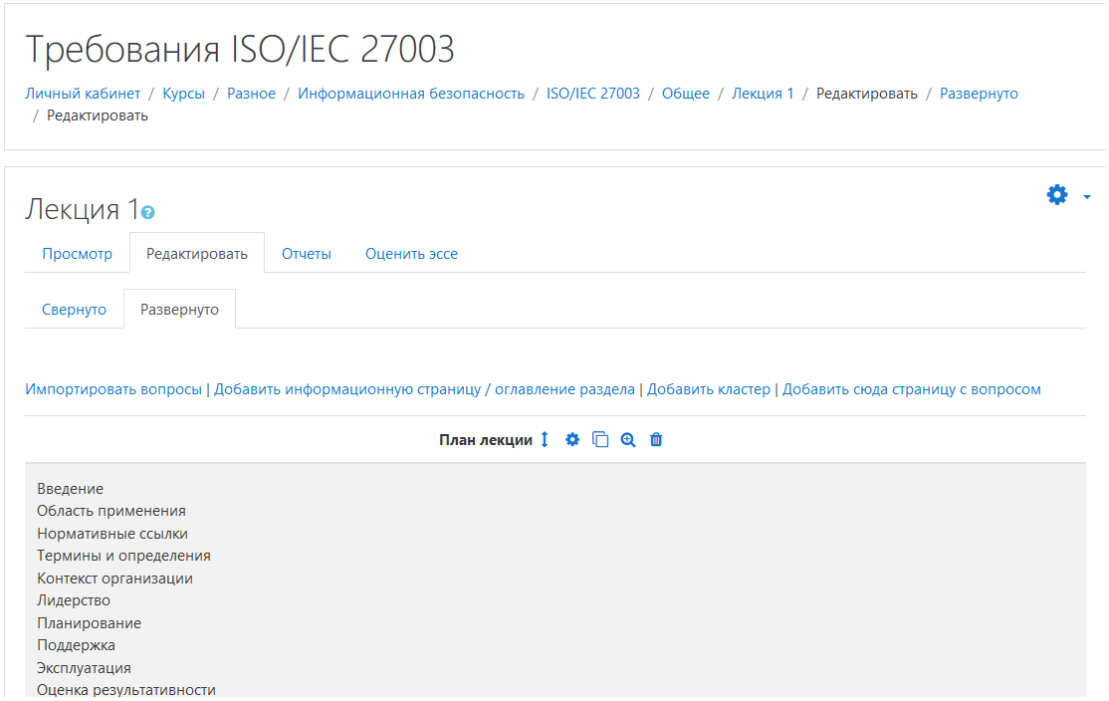

Рисунок 2.18 – Редактирование лекции

В рамках редактирования курса, администратор может добавлять тестовые задания для контроля. Для тестового задания можно устанавливать проходной балл, лимит времени и другие настройки. Тест наполняется вопросами одного или нескольких различных типов, представленных на рисунке 2.19.

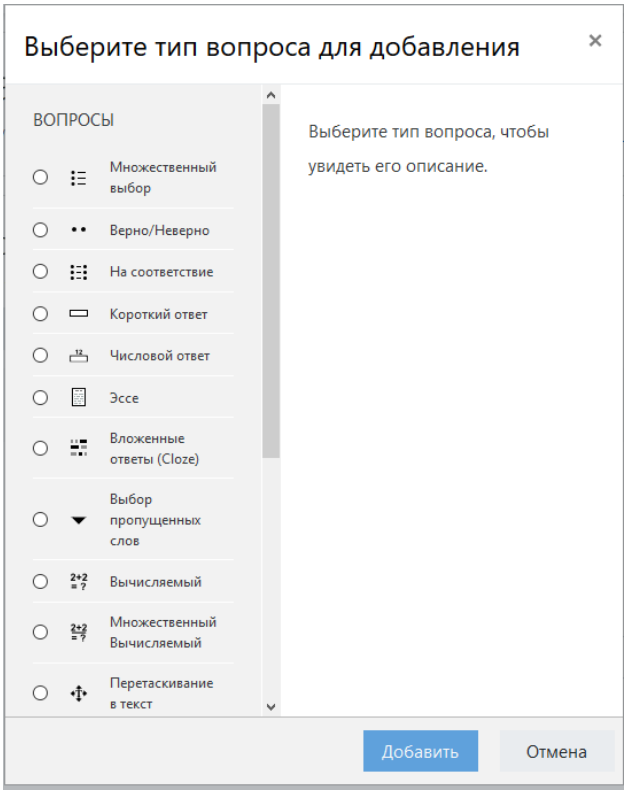

Рисунок 2.19 – Виды вопросов, поддерживаемых в тестах

Также администратору доступен отчёт по оценкам, позволяющий контролировать прохождение курсов. Если оценка пользователя за тест превышает пороговое значение, цвет оценки будет зелёным, в противном случае красным. Пример отчёта по оценкам представлен на рисунке 2.20.

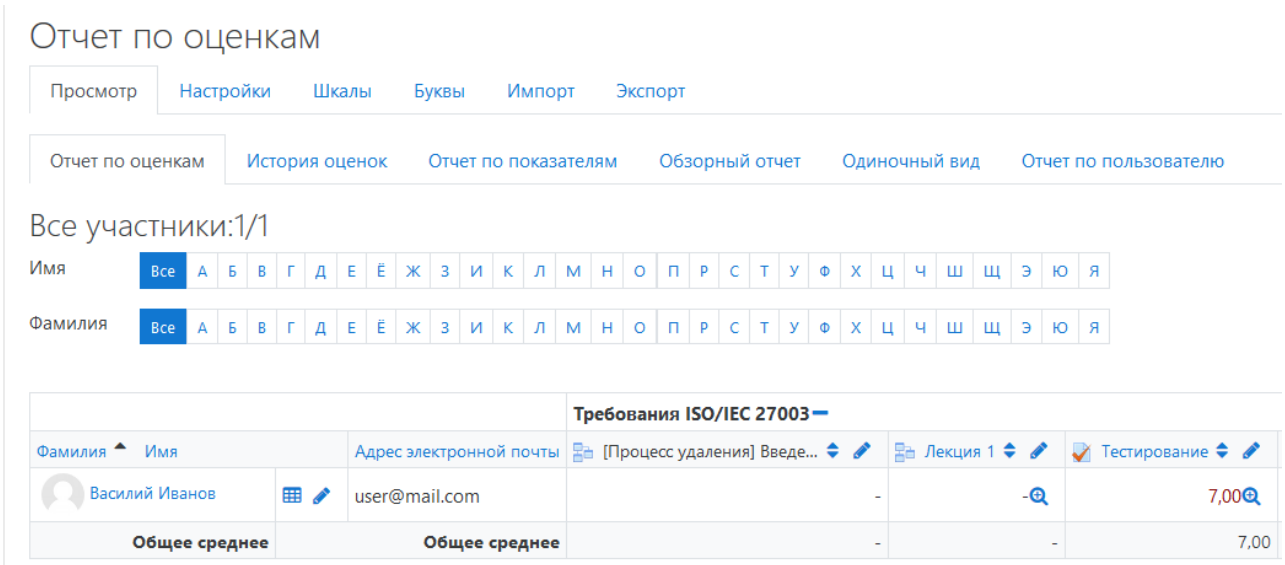

Рисунок 2.20 – Отчёт по оценкам

Стоит отметить, что это лишь небольшая часть всех возможностей платформы Moodle, и в дальнейшем используемая функциональность может быть значительно расширена.

Таким образом, в данном параграфе приводится контрольный пример реализации всех функций приложения.

2.7 Тестирование системы обучения

Для проверки корректности внедрения системы было проведено функциональное и нефункциональное тестирование. Функциональное тестирование используется для того, чтобы удостовериться в корректной работе системы с точки зрения предоставляемых функций. В рамках функционального тестирования были проведены следующие тесты:

- компонентное тестирование – процесс проверки компонентов системы. Были проверены модуль тестирования и модуль создания учебных курсов. Было проверено, что администратор системы может создавать курсы, устанавливать критерии оценки и при прохождении пользователем данного тестирования система работает ожидаемо. Проверка проводилась через веб браузер Google Chrome путём ручного тестирования;
- интеграционное тестирование – процесс проверки взаимодействия с имеющимися ИТ системами компании, такими как почтовый сервер для отправки уведомлений. В ходе данного тестирования было проверено, что система корректно отправляет почтовые уведомления. Проверка проводилась путём отправки сообщения администратору курса после успешного прохождения пользователем тестирования.

Нефункциональное тестирование подтвердило соответствие нефункциональным требованиям к системе, таким как быстродействие и отказоустойчивость. В рамках данного вида проверок было проведено нагрузочное тестирование системы на аппаратном обеспечении в конфигурации, указанной в нефункциональных требованиях к системе. После

этого следует была проведена эмуляция работы пользователей, исходя из максимального предполагаемого количества пользователей, использующих систему одновременно (2000 пользователей при общей численности 1600 сотрудников в России) с помощью приложения JMeter. Среднее время отклика системы составило 73 мс. В процессе нагрузочного тестирования была выявлена ошибка нехватки ОЗУ под нагрузкой по причине того, что интерпретатор PHP по умолчанию имеет лимит потребляемого ОЗУ в 64 Мб. Текст ошибки представлен на рисунке 2.21.

```
Fatal error: Allowed memory size of 67108864 bytes exhausted
(tried to allocate 22760 bytes) in /var/www/moodle/index.php
```

Рисунок 2.21 – ошибка PHP при нагрузочном тестировании

Это известная проблема, описанная в документации. Для исправления проблемы был изменён лимит путём редактирования файла php.ini на веб сервере, установив лимит в 1 Гб: «memory_limit = 1024M».

Выводы по главе 2

В рамках данной главы приводится описание процессов внедрения и наполнения информационной системы.

На первом этапе была получена логическая модель, характеризующая сущности и их взаимоотношения. Сущностями рассматриваемой предметной области являются:

- сотрудники;
- учебные предметы;
- тесты.

Нормативно-справочной информацией разрабатываемой системы является стандарт ISO/IEC 27001 – Менеджмент информационной безопасности.

Этап физического моделирования служит для обеспечения на экспериментальном уровне проверки реальной работоспособности созданной логической модели.

Система работает в интерактивном режиме через веб интерфейс. Вся информация об учебных курсах, тестах и результатах их прохождения хранится в базе данных.

Также в данной главе приводится контрольный пример реализации проекта, отображающий функционирование всех элементов и описывается процесс тестирования после внедрения с целью удостовериться в корректности работы системы.

Глава 3 Оценка и обоснование экономической эффективности проекта внедрения корпоративной системы обучения сотрудников

3.1 Выбор и обоснование методики расчета экономической эффективности

Для обоснования экономической эффективности работы могут применяться следующие методики:

- расчет прямой эффективности от внедрения информационной системы по сравнению с базовым вариантом существующей организации обработки информации;
- расчет экономической эффективности, исходя из жизненного цикла проекта разработки и внедрения подсистем корпоративной ИС.

Первая методика не может быть использована в силу отсутствия базового аналога разработанного программного продукта для тестирования знаний по информационной безопасности сотрудниками компании Deutsche Telekom.

Экономическая эффективность разработки определяется двумя параметрами:

- прямым эффектом – заключается в снижении трудовых, стоимостных показателей за счет уменьшения времени получения и обработки данных, сокращения трудоемкости работы и стоимостных затрат обработки документов, повышении точности и достоверности информации, а также степени ее защищенности. Для расчета прямого эффекта от внедрения разработанного программного продукта необходимо опираться на показатели трудовых и стоимостных затрат;
- косвенным эффектом – заключается в увеличении прибыли, привлечении большего количества клиентов, снижении уровня брака в производстве, уменьшении числа рекламаций клиентов, снижении затрат на сырье и материалы, уменьшении сумм штрафов, неустоек и т. д.

В данном случае эффективность от внедрения заключается в увеличении показателей безопасности данных внутри компании, что оказывает влияние на ее имидж на мировом рынке.

К наиболее популярным методикам оценки защиты информации относятся:

- прикладной информационный анализ Applied Information Economics (AIE) – данная методика разработана Дугласом Хаббардом с целью анализа ценности инвестиций в технологии безопасности с экономической и финансовой точек зрения. Использование методики AIE приводит к сокращению неопределенности затрат, рисков и выгод, в том числе и неочевидных. Опираясь на знания статистики, экономики, теории информации и системного анализа, выявляются финансовые показатели на базе дополнительных сведений, что позволяет уменьшить их неопределенность, а также оценить влияние рисков и выбрать такую стратегию, которая сократит риск и оптимизирует инвестиционные вложения [3];
- потребительский индекс Customer Index (CI) – в данной методике предлагается оценка степени влияния инвестиций в технологии безопасности по отношению к численности и составу потребителей. В процессе оценки компания определяет перечень экономических показателей своих потребителей путем отслеживания доходов и затрат по каждому заказчику в отдельности. Недостатком данной методики является трудность формализации процесса установления прямой связи между инвестициями в технологии безопасности и сохранением или увеличением количества потребителей. Чаще всего методика используется для оценки эффективности корпоративных систем защиты информации в компаниях, число заказчиков которых непосредственно влияет на все аспекты бизнеса [7];
- добавленная экономическая стоимость Economic Value Added (EVA) – данная методика предлагает рассматривать службу информационной безопасности как «государство в государстве». Другими словами - специалисты

службы безопасности продают свои услуги внутри компании по ценам, примерно равным ценам на внешнем рынке, что позволяет компании отслеживать доходы и расходы, связанные с технологиями безопасности. Таким образом, служба безопасности является центром прибыли, позволяя при этом определять, как расходуются активы, связанные с технологиями безопасности, и увеличиваются доходы акционеров.

На практике вопрос обеспечения защиты информации решается в условиях случайного воздействия различных факторов. Часть факторов определена установленными стандартами, а часть заранее неизвестна, в результате чего способна оказывать негативное влияние на эффективность существующих мер.

Оценка эффективности защиты должна обязательно учитывать не только объективные обстоятельства, но и вероятностные факторы.

Экономическим эффектом называется конкретный результат экономической деятельности вне зависимости от затрат.

Экономическая эффективность – результативность деятельности, соотношение доходов и расходов, а также сопоставление результатов и затрат на их достижение.

Принято выделять два вида экономической эффективности:

- абсолютную – определяется соотношением результатов экономической деятельности и затрат, необходимых для достижения этих результатов;
- сравнительную – показывает изменение результатов экономической деятельности по отношению к уже достигнутым результатам [13].

Но сохраняется фундаментальная проблема, а именно достаточность и эффективность систем защиты с точки зрения пользователя. Чаще всего в качестве показателя потребительских качеств подобных систем выступает соотношение «стоимость/эффективность», т.е., в конечном счете, баланс между возможным ущербом от несанкционированных действий и размером вложений,

которые необходимо потратить для обеспечения защищенности информационных ресурсов.

Инвестиции в разработку проектов защиты объекта, закупку необходимых элементов безопасности и эксплуатацию систем защиты для владельца информации есть ничто иное, как материализованный экономический ущерб. Идя на эти траты, руководитель надеется избежать большего ущерба, связанного с возможным нарушением конфиденциальности.

Если стоимость средств защиты информации (СЗИ) по сравнению с предполагаемым ущербом мала, основным фактором риска в данном случае являются экономические потери, вызванные несанкционированными действиями. В противном случае потери будут связаны с чрезмерно высокой стоимостью разработки.

Также важно отметить, что затраты на СЗИ носят детерминированный характер, поскольку они уже материализованы в конкретные меры, способы и средства защиты, а возможный ущерб является случайной величиной [14].

В качестве меры риска понимаются ожидаемые суммарные потери в процессе защиты информации в течение определенного промежутка времени. Моделирование риска собственника информации при создании и эксплуатации СЗИ реализуется на базе функциональных зависимостей между риском R, стоимостью СЗИ - S, вероятностью преодоления СЗИ и нанесения ущерба собственнику – p, а также размером возникающего при этом ущерба - U.

Типичный пример зависимости уровня риска от стоимости СЗИ, полученный при условии того, что вероятность нанесения ущерба p уменьшается с ростом стоимости системы S (т.е. соответствующая производная отрицательна, $p/s < 0$) приведена на рисунке 3.1.

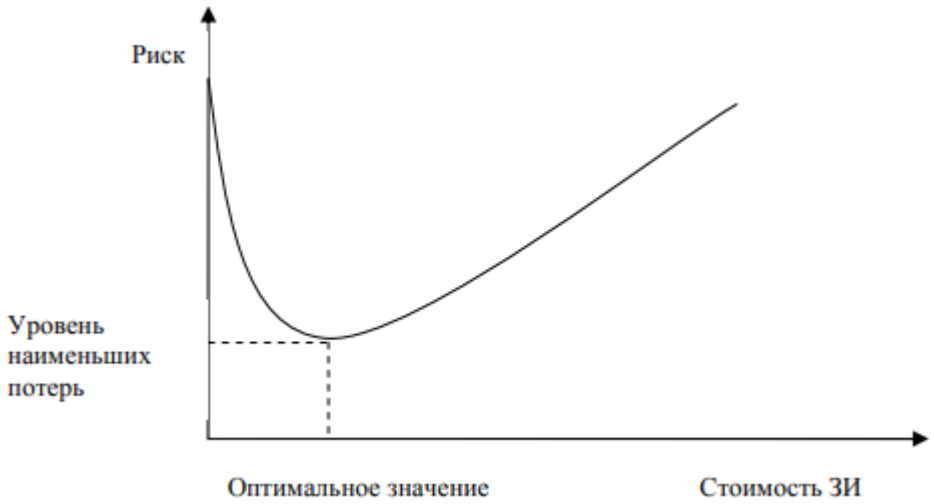

Рисунок 3.1 - Зависимость уровня риска от стоимости СЗИ (p/S < 0)

Анализ данной зависимости показывает, что даже использование недорогих СЗИ способно резко снизить суммарные потери компании.

Таким образом, вложение даже малых средств в СЗИ является очень эффективным. При некоторой стоимости СЗИ риск имеет наименьшее значение. Данная величина является оптимальной.

Дальнейший, сверх оптимального значения, рост затрат на СЗИ будет вести к увеличению экономических потерь собственника информации. Его выигрыш в повышении надежности системы защиты и соответствующем снижении вероятности ущерба от несанкционированных действий будет нивелироваться и обесцениваться чрезвычайно высокой стоимостью самой СЗИ.

Поэтому лучшей стратегией является использование СЗИ, обеспечивающих минимум риска.

На рисунке 3.2. представлена зависимость вероятности несанкционированных действий с защищаемой информацией при оптимальной СЗИ от величины ущерба.

Таким образом, основой определения эффективности защиты информации является сопоставление отношения доходов и расходов.

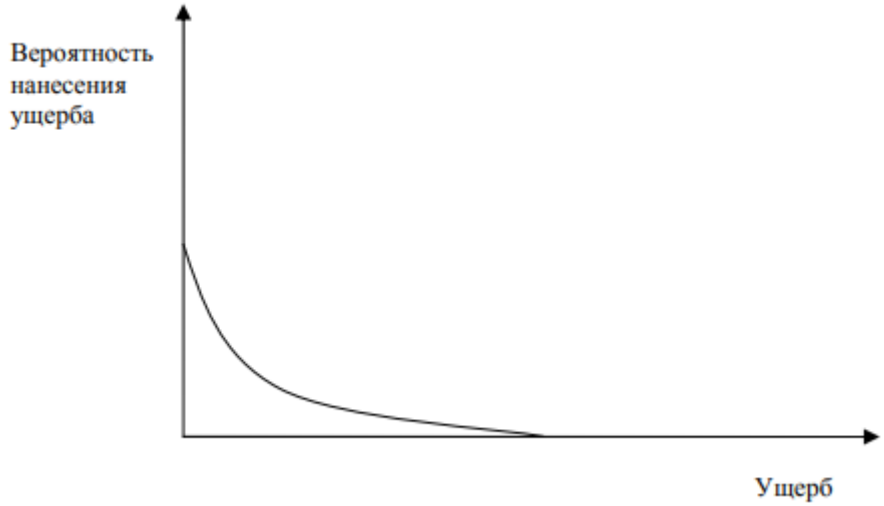

Рисунок 3.2 - Зависимость вероятности несанкционированных действий в оптимальности СЗИ от размера возможного ущерба

Экономическая эффективность внедрения разработанного продукта может быть определена через объем предотвращенного ущерба или величину снижения риска для информационных активов компании.

Для того чтобы воспользоваться данным подходом к решению проблемы, необходимо знать:

- ожидаемые потери при нарушении защищенности информации;
- зависимость уровня защищенности и средств, затрачиваемых на защиту информации.

Для определения уровня затрат R_i, обеспечивающих требуемый уровень защищенности информации, необходимо знать:

- полный перечень угроз информации;
- потенциальную опасность для информации для каждой из угроз;
- размеры затрат, необходимых для нейтрализации каждой из угроз.

В силу того, что оптимальное решение вопроса о целесообразном уровне затрат на защиту определяется уровнем ожидаемых потерь при нарушении защищенности, достаточно определить только уровень потерь. В качестве одной из методик определения уровня затрат возможно использование

следующей эмпирической зависимости ожидаемых потерь (рисков) от i-й угрозы информации: $R_i = 10^{(S_i + V_i - 4)}$ где:

- S_i – коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы;
- V_i – коэффициент, характеризующий значение возможного ущерба при ее возникновении.

Таким образом, оценив величину зависимости потерь, можно сделать вывод о целесообразности внедрения СЗИ [11].

Таким образом, в данном параграфе приводится описание методики расчета экономической эффективности проекта.

3.2 Расчет показателей экономической эффективности проекта

Для расчета показателей экономической эффективности используются следующие виды угроз:

1. предумышленное предоставление конфиденциальной информации сотрудниками компании третьим лицам;

2. непредумышленное предоставление конфиденциальной информации сотрудниками компании третьим лицам.

Согласно информации от компании Deutsche Telekom исходные данные для расчета рисков по данным угрозам следующие:

- $S_1 = 3$ (1 раз в 3 года, и реже, чем 1 раз в год);
- $V_1 = 8$ (более 2 млн. руб.);
- $S_2 = 5$ (1 раз в месяц, примерно 10 раз в год);
- $V_2 = 4$ (300 тыс. руб.).

Подставив эти значения в формулу 3.1 получим:

$R_1 = 10^{(3+8-4)} = 10^7$ руб. = 10.000.000 руб.

$R_2 = 10^{(5+4-4)} = 10^5 = 100.000$ руб.

$R = R_1 + R_2 = 10.100.000$ руб.

Затраты компании, необходимые на внедрение программного продукта, представлены в таблице 3.1.

Таблица 3.1 - Затраты на внедрение

Статья расходов	Величина	Комментарий
Среднечасовая заработная плата	568 руб.	Из расчета оклада в 100 тыс. руб.
Время на внедрение и тестирование	96 часов	12 рабочих дней
Серверная инфраструктура в облаке Microsoft Azure	40 000 руб.	Linux сервер с Apache, PHP и PostgreSQL
Среднечасовая заработная плата инженера по защите информации	682 руб.	Из расчета оклада в 120 тыс. руб.
Время инженера на создание и наполнение курса	12 часов	2 рабочих дня

Таким образом, затраты на внедрение проекта составляют:

S = 568*96 + 40000 + 12*682 = 102 712 руб.

Анализ возможных угроз говорит о том, что разработанный проект позволит снизить величину угроз второго типа - непредумышленное предоставление конфиденциальной информации сотрудниками компании третьим лицам, убыток от которого составляет 300 тыс. руб. в год.

Очевидно, что сумма, затраченная на внедрение проекта существенно меньше суммы убытков, вызванных человеческим фактором незнания правил информационной безопасности, следовательно, проект эффективен.

Таким образом, в данном параграфе приводится расчет показателей экономической эффективности проекта.

Выводы по главе 3

В рамках данной главы рассмотрены существующие методики анализа и оценки эффективности средств защиты информации, а также проведен анализ внедрения программного продукта, доказывающий эффективность проделанной работы.

Заключение

В рамках выполнения данной ВКР рассмотрена тема «Разработка проекта внедрения системы корпоративного обучения сотрудников Deutsche Telekom».

В первой главе работы приводится анализ предметной области «информационная безопасность» компании Deutsche Telekom. Компания Deutsche Telekom является крупнейшим провайдером телекоммуникационных услуг на территории Германии. Полный спектр предоставляемых услуг очень широк: начиная от консалтинга, проектирования, разработки, внедрения и интеграции, и заканчивая управлением жизненным циклом приложений и хостингом. Одним из слабых мест компании Deutsche Telekom является первичное обучение сотрудников основам информационной безопасности, что подтверждается периодическим возникновением инцидентов ИБ.

Существующая политика безопасности внутри компании не предусматривала тестирования сотрудников. Поэтому некоторые из были знакомы в достаточной мере с корпоративными требованиями и регламентами по информационной безопасности. Задачей данной выпускной квалификационной работы являлось внедрение автоматизированной системы обучения сотрудников компании Deutsche Telekom.

Во второй главе работы описана разработка проектных решений по обучению сотрудников. Произведено логическое и физическое моделирование предметной области, описаны существующие решения, проведён их анализ и выбор оптимального из них. В качестве решения для внедрения была выбрана платформа с открытым исходным кодом Moodle. Также в ней приводится описание модулей приложения и контрольный пример работы с платформой, в ролях пользователя и администратора.

Третья глава работы отражает оценку и обоснование экономической эффективности проекта. Экономическая эффективность внедрения разработанного продукта может быть определена через объем предотвращенного ущерба или величину снижения риска для информационных

активов компании. Анализ возможных угроз говорит о том, что разработанный проект позволит снизить величину угроз второго типа - непредумышленное предоставление конфиденциальной информации сотрудниками компании третьим лицам, убыток от которого в настоящее время составляет 300 тыс. руб. в год.

Список использованной литературы

1. Ахметшин Д.А. Проектирование информационных систем / Д.А. Ахметшин, Н.К. Нуриев, С.Д. Старыгина, З.Х. Шакирова. – Казань: Отечество, 2016. – 172 с.

2. Баканов М.В. Базы данных. Системы управления базами данных: учебное пособие / М.В. Баканов, В.В. Романова, Т.П. Крюкова. Кемеровский технологический институт пищевой промышленности. – Кемерово, 2010. – 166 с.

3. Балдин К.В. Информационные системы в экономике / К.В. Балдин, В.Б. Уткин. – М.: Дашков и К, 2015. – 395 с.

4. Вайсфельд М. Объектно-ориентированное мышление. – СПб.: Питер, 2014. – 304 с.

5. Варфоломеева А.О. Информационные системы предприятия / А.О. Варфоломеева, А.В. Коряковский, В.П. Романов. – М.: НИЦ ИНФРА-М, 2013. – 283 с.

6. Войтик А.И. Экономика информационной безопасности. – СПб.: НИУ ИТМО, 2012. – 120 с.

7. Громов Ю.Ю. Технология программирования / Ю.Ю. Громов, О.Г. Иванова, М.П. Белев, Ю.В. Минин. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 172 с.

8. Долженко А.И. Управление информационными системами. – Ростов-на-Дону: Изд-во РГУ, 2017. – 191 с.

9. Евгенев Г.Б. Основы автоматизации технологических процессов и производств / Г.Б. Евгенев, С.С. Гаврюшин, А.В. Грошев, М.В. Овсянников, П.С. Шильников. – Москва: Изд-во МГТУУ им. Н.Э. Баумана, 2015. – 441 с.

10. Ковецкий Е.В. Проектирование структуры VPN сети предприятия. – Новосибирск: Изд-во СибГУТИ, 2016. – 148 с.

11. Краснянский М.Н. Проектирование информационных систем управления документооборотом научно-образовательных учреждений / М.Н.

Краснянский, С.В. Карпушкин, А.В. Остроух. – Тамбов: Изд-во ФГБОУ ВПО ТГТУ!, 2015. – 216 с.

12. Куликов Г.Г. Автоматизированные информационные системы в экономике: учебное пособие / Г.Г. Куликов, Е.А. Дронь, М.А. Шилина, Ю.О. Багаева. – Уфа: УГАТУ, 2013. – 186 с.

13. Михеева Е.В. Информатика / Е.В. Михеева, О.И. Титова. – М.: Издательский центр «Академия», 2014. – 352 с.

14. Мокеев В.В. Бизнес-информатика / В.В. Мокеев, Е.В Бунова, О.С. Буслаева. – Челябинск: издательский центр ЮУрГУ, 2015. – 67 с.

15. Одинцов Б.Е. Информационные системы управления эффективностью бизнеса. - Люберцы: Юрайт, 2015. - 206 с.

16. Рудаков А.В. Технология разработки программных продуктов. – М.: Академия, 2014. – 190 с.

17. Юрченко Т.В. Информационные системы в экономике и управлении: учебное пособие. – Н.Новгород: ННГАСУ, 2013. – 114 с.

Источники на иностранном языке:

18. Don Watkins, Education management with Moodle: The beginning, the middle and today // opensource.com, 2016. URL: https://opensource.com/life/16/11/moodle-today (дата обращения: 18.05.2018)

19. Brett Henebery, Big things on the horizon for edutech giant // theeducatoronline.com, 2016. URL: https://www.theeducatoronline.com/au/news/big-things-on-the-horizon-for-edutech-giant/226070 (дата обращения: 18.05.2018)

20. Don Murdoch, 2014. Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder. Create Space Independent Publishing Platform, 2014.

21. Caroline Wong, 2011. Security Metrics, A Beginner's Guide. McGraw-Hill Education, 2011.

22. Corey Schou, 2014. Information Assurance Handbook: Effective Computer Security and Risk Management Strategies. McGraw-Hill Education, 2014.

Приложение А Список сокращений

АИС – автоматизированная информационная система

АИТ – автоматизированная информационная технология

БД – база данных

ИБ – информационная безопасность

ИС – информационная система

ИТ – информационные технологии

СБ – система безопасности

СЗИ – средства защиты информации

СУБД – система управления базой данных

ЭВМ – электронно-вычислительная машина