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

СИСТЕМА ТЕСТИРОВАНИЯ ДЛЯ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ НА ОСНОВЕ МЕЖДУНАРОДНЫХ СТАНДАРТОВ

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: 189

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

СИСТЕМА ТЕСТИРОВАНИЯ ДЛЯ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ НА ОСНОВЕ МЕЖДУНАРОДНЫХ СТАНДАРТОВ

Исполнитель: И. Е. Филиппов
обучающийся группы № ИБ-401
Руководитель:
ст. преподаватель каф. ИС С. В. Ченушкина
Нормоконтролер: Т. В. Рыжкова

Екатеринбург 2018

АННОТАЦИЯ

Выпускная квалификационная работа состоит из разработанного веб-приложения и банка вопросов, а также из доработанного плагина тестирования и пояснительной записки на 73 страницах, содержащей 32 рисунка, 3 таблицы, 38 источников литературы и 2 приложений на 5 страницах.

Ключевые слова: АУДИТ, ОЦЕНКА РИСКОВ, АНАЛИЗ УГРОЗ.

Филиппов И.Е., Система тестирования для проведения аудита информационной безопасности на предприятии на основе международных стандартов: выпускная квалификационная работа / И. Е. Филиппов; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2018. — 73 с.

Принимая во внимание тот факт, что с каждым годом возрастает количество атак на предприятия, наносящие им значительный финансовый и материальный урон, становится актуальной проблема, изучением и работой над которой занимаются большое количество фирм, формирующие собственный рынок по услугам объективной оценки состояния уровня безопасности информационных систем.

Актуальность и новизна выбранной темы заключается в том, что современных аналогов продукту нам найти не удалось, за исключением системы Кондор, которая была основана на устаревшем стандарте ISO 17799 и прекратила поддержку в 2008 году по инициативе руководства компании.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современный мир уже невозможно представить без персональных компьютеров, высокоскоростного Интернета и прочих современных девайсов, с которыми люди взаимодействует каждый день. Они становятся неотъемлемыми атрибутами, которые сопровождают человека в повседневной жизни, как в быту, так и на рабочем месте. Все процессы в современном обществе перетекают в информационные системы, которые играют ключевую роль в обеспечении эффективности работы коммерческих, государственных предприятий и образовательных организаций. Повсеместное использование информационных систем, которые привлекаются для хранения, обработки и передачи информации, обуславливает актуальность проблемы защиты и сохранности информации.

Принимая во внимание тот факт, что с каждым годом возрастает количество атак на предприятия, которые наносят значительный финансовый и материальный урон, становится актуальной еще одна проблема, изучением и работой над которой на сегодняшний день занимаются большое количество фирм, тем самым формируя собственный рынок, со своей конкуренцией и правилами, которые предлагают услуги по объективной оценке состояния уровня безопасности информационной системы, действующей политики информационной безопасности на предприятии. Услуги данных фирм привлекаются для проведения какого-либо одного из существующих видов аудита информационной безопасности, так и для проведения комплексного аудита систем безопасности на предприятии, по результатам которого выдается комплексное заключение о выявленных рисках и практические рекомендации по их предотвращению и предупреждению.

Исходя из вышеизложенных соображений, следует считать, что тема выпускной квалификационной работы «Система тестирования для проведения аудита информационной безопасности на предприятиях на основе стандартов

ISO/IEC 27002 и ISO/IEC 15408» является актуальной в силу того, что потребность в такой разработке существует.

Объект исследования — использование международных стандартов в области информационной безопасности для разработки и внедрения организациями системы менеджмента информационной безопасности, в контексте выбора, внедрения, улучшения мер безопасности и управления имеющимися рисками.

Предмет исследования — банк тестовых вопросов на основе рекомендаций международных стандартов ISO/IEC 27002 и ISO/IEC 15408 для проведения аудита информационной безопасности на предприятии на предмет оценки и анализа существующих рисков.

Цель выпускной квалификационной работы — разработать систему тестирования для проведения аудита информационной безопасности на предприятии на предмет оценки рисков на основе данных международных стандартов ISO/IEC 27002 и ISO/IEC 15408.

Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать литературу и интернет-источники по аудиту и менеджменту информационной безопасности;
- изучить международные стандарты информационной безопасности, для подготовки исходных данных и составления тестовых вопросов;
- подготовить банк тестовых вопросов по выбранным международным стандартам информационной безопасности;
- реализовать интерфейс для проведения интернет-тестирования с возможностью авторизованного доступа и вывода результатов;
- разработать интернет-сайт для представления результата работы над продуктом в среде Интернет и обеспечение доступа представителям различных организаций.

1 АКТУАЛЬНОСТЬ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

1.1 Основные риски в области информационной безопасности

Сфера информационной безопасности образовалась, получила широкое развитие и всеобщую популяризацию в связи с постоянно растущим числом информационных атак в совокупности с необходимостью защиты от них и всевозможных рисков. Само по себе, определение риска информационной безопасности можно обобщенно рассматривается как возможность того, что может произойти определенное неблагоприятное событие, имеющее определенный размер наносимого ущерба и ожидаемую вероятность наступления с негативными последствиями [27]. Основными рисками информационной безопасности являются:

- риск утечки конфиденциальной информации;
- риск потери и/или недоступности важных данных;
- риск нарушения целостности информации и/или важных данных;
- риск неправомочной эксплуатации информационных ресурсов;
- риск распространения дискредитирующей во внешней среде информации, угрожающей репутации организации и т. п. [27].

Основными видами угроз безопасности, рассматриваемыми при проведении аудита информационной безопасности, являются [37]:

1. Организационные (законодательные, административные, процедурные), например:

- отсутствие контроля и/или неэффективно применяемые меры управления такими процессами как: управление конфигурациями, управление изменениями, управление обновлениями и т. д.;
- атаки через привлекаемые подрядные организации и т. п.

2. Эксплуатационные, например:

- неподдерживаемые и/или нелицензионные версии операционных систем, системного программного обеспечения, программных продуктов;
- уязвимости веб-серверов и/или использование небезопасных протоколов управления (использование SSL и TLS может привести к перехвату передаваемой информации об аутентификации) и передачи информации;
- слабые пароли и/или недостаточно проработанная парольная политика в организации и т. п.

3. Программно-технические (архитектурные), например:

- возможность подключения корпоративных устройств к незащищенным сегментам гостевых беспроводных сетей компании;
- неконтролируемые информационные потоки и т. п.

4. Прочие аспекты обеспечения информационной безопасности, которые необходимо учесть в ходе проведения аудита, для определения их приоритетов.

1.2 Описание терминологии и виды аудита информационной безопасности

Говоря об аудите информационной безопасности стоит знать и разводить значение двух терминов: информационная безопасность и аудит информационной безопасности.

Информационная безопасность — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере [12].

Аудит информационной безопасности — системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности [12].

Связав оба термина, на выходе можно получить обобщенное определение аудита информационной безопасности, рассматриваемое как процесс сбора и анализа информации об информационной системе для качественной и количественной оценки уровня ее защищенности от атак злоумышленников.

Основными целями и задачами при проведении аудита информационной безопасности являются [7, 9, 10, 12]:

1. Цели аудита информационной безопасности:

- анализ рисков информационной безопасности, которые напрямую связаны с возможностью осуществления угроз безопасности для предприятия в отношении ресурсов информационной системы;
- оценка текущего состояния уровня защищенности информационной системы предприятия;
- определение «узких мест» в системе безопасности информационной системы предприятия;
- оценка информационной системы предприятия на предмет соответствия существующим стандартам и нормативно-правовым документам в области информационной безопасности;
- разработка рекомендаций по внедрению новых и/или повышению эффективности существующих механизмов безопасности информационной системы предприятия.

2. Задачи аудита информационной безопасности:

- разработка политик безопасности и/или других организационно-распорядительных документов по защите информации на предприятии, участие в их внедрении в работу предприятия;
- постановка задач для персонала предприятия, занятого в сфере информационных технологий и информационной безопасности предприятия, касающихся обеспечения защиты информации, участие в их обучении;

- участие в обучении пользователей и обслуживающего персонала информационной системы вопросам обеспечения информационной безопасности на предприятии;
- участие в разборе и анализе инцидентов, связанных с нарушением информационной безопасности и др.

Основные направления аудита информационной безопасности [12]:

1. Аттестация объектов информатизации по требованиям стандартов и другой нормативной документации в области информационной безопасности, например:
   - аттестация автоматизированных систем, средств связи, обработки и передачи информации;
   - аттестация помещений, предназначенных для ведения конфиденциальных переговоров;
   - аттестация технических средств, установленных в выделенных помещениях и т. п.
2. Контроль защищенности информации ограниченного доступа, например:
   - выявление технических каналов утечки и способов несанкционированного доступа к информации;
   - контроль эффективности применяемых средств защиты и т. п.
3. Специальные исследования технических средств на наличие побочных электромагнитных излучений и наводок, например:
   - исследование персональных компьютеров, средств связи и обработки информации;
   - исследование локальных вычислительных систем;
   - оформление результатов исследований в соответствии с требованиями Гостехкомиссии Российской Федерации (РФ) и т. п.

4. Проектирование и разработка систем, документации по обеспечению информационной безопасности компании, например:

- разработка концепции информационной безопасности;
- проектирование автоматизированных систем, средств связи, обработки и передачи информации в защищенном исполнении;
- проектирование помещений, предназначенных для ведения конфиденциальных переговоров и т. п.

Аудит безопасности предприятия — нужный и полезный процесс, особенно для крупных компаний. В основном он крайне необходим на этапе подготовки технического задания по проектированию систем защиты информации и/или после внедрения системы безопасности для оценки уровня ее эффективности. Также, аудит информационной безопасности проводится на приведение действующей системы безопасности в соответствие требованиям, предъявляемым законодательством РФ, и/или международным законодательством, и/или требованиям нормативной документации в области информационной безопасности. Помимо этого, целесообразно проводить аудит информационной безопасности на предприятии в случае если необходимо систематизировать и/или упорядочить существующие меры защиты информации или расследовать произошедший инцидент, связанный с нарушением установленного режима информационной безопасности на предприятии.

Проведение аудита информационной безопасности в компании-заказчике включает в себя ряд последовательных этапов [9]:

1. Инициирование процедуры аудита.
2. Сбор информации, необходимой для проведения аудита.
3. Анализ данных аудита.
4. Формирование и составление рекомендаций.
5. Подготовка аудиторского отчета.

Инициирование процедуры аудита. Зачастую инициатором проведения аудита информационной безопасности становится руководство компании, ко-

торое в наибольшей степени заинтересовано в его проведении. Аудит информационной безопасности на предприятии — довольно длительный, трудоемкий и всеобъемлющий процесс, в который оказываются вовлечены многие, если не все структурные подразделения и сотрудники компании, поэтому на этапе инициирования процедуры аудита должны быть решены следующие организационные вопросы [9]:

- должны быть четко определены и документально закреплены права и обязанности аудитора в его должностных инструкциях, а также в положении о проведении аудита компанией-аудитором в компании-заказчике;
- аудитором должен быть составлен и согласован с руководством компании-заказчика план проведения аудита;
- в положении о проведении аудита компанией-аудитором в компании-заказчике должно быть документально закреплено, что сотрудники компании-заказчика должны оказывать содействие аудитору (группе аудиторов) и предоставлять всю необходимую информацию;
- должны быть определены границы проведения аудита (касаемо всех систем и подсистем компании-заказчика, которые могут быть недоступны для проверки из-за соображений конфиденциальности): список обследуемых физических, программных, информационных ресурсов и помещений компании, попадающих под проверку.

Сбор информации аудита. Данный этап проведения аудита является наиболее длительным и сложным, но это целиком зависит от того, насколько полно и своевременно аудитор получает необходимую для проверки документацию, а также, насколько плотно происходит взаимодействие аудитора с должностными лицами компании-заказчика и лицами, уполномоченными помогать аудитору. Компетентные выводы относительно текущего состояния уровня защищенности и имеющихся рисков в компании-заказчике могут быть сделаны аудитором только при условии наличия всей необходимой для анализа документации. Получение информации о принятых в компании процедурах

информационной безопасности, о функционировании и текущем состоянии информационной системы осуществляется аудитором в ходе специально проводимого интервьюирования ответственных лиц компании, а также путем изучения технической, организационно-распорядительной документации и исследования информационной системы с помощью специализированных программных средств. Аудитору может потребоваться следующая организационно-распорядительная документация для анализа [9]:

- описание автоматизированных функций;
- описание основных технических решений;
- схема организационной структуры пользователей;
- схема организационной структуры обслуживающих подразделений;
- различные функциональные схемы;
- другая проектная и рабочая документация на информационную систему компании-заказчика.

Анализ данных аудита. Используемые аудиторами методы анализа данных определяются на основании выбранного подхода к проведению аудита, которые могут существенно различаться [9].

Первый подход базируется на анализе рисков. Опираясь на методы анализа рисков, аудитор определяет для обследуемой информационной системы индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной информационной системы, среды ее функционирования и существующие в данной среде угрозы безопасности. Данный подход является наиболее трудоемким и требует высокой квалификации аудитора. В данном случае на качество результата аудита может сильно повлиять используемая методика анализа и управления рисками, а также степень ее применимости к данному типу информационной системы.

Второй подход основан на использовании стандартов информационной безопасности. Используемыми стандартами определяется базовый набор требований безопасности к определенному классу информационных систем, который

формируется в результате обобщенной мировой практики. Стандарты могут определять разные наборы требований безопасности, в зависимости от уровня защищенности информационной системы, которые требуется обеспечить, в зависимости от ее принадлежности (коммерческая организация, государственное учреждение и т. п.), а также назначения (финансы, промышленности, связь и т. п.). В данном случае от аудитора требуется правильно определить набор требований стандарта, соответствие которым требуется обеспечить для данной информационной системы. Также, необходимо правильно выбрать методику, которая позволит оценить это соответствие. Из-за своей простоты (поскольку стандартный набор требований для проведения аудита уже определен стандартом) и надежности (стандарт - есть стандарт и его требования не оспоримы), описанный подход наиболее распространен на практике (особенно при проведении внешнего аудита). Данный подход при минимальных затратах на ресурсах позволяет сформировать обоснованные выводы о текущем состоянии уровня безопасности информационной системы.

Третий подход предполагает комбинирование первых двух, поэтому является наиболее эффективным. Базовый набор требований безопасности, предъявляемых к информационной системе, определяется стандартом. Дополнительные требования, в максимальной степени учитывающие особенности функционирования данной информационной системы, формируются на основе анализа рисков. Этот подход является намного проще первого, так как большая часть требований безопасности уже определена стандартом, и, в то же время, он лишен недостатка второго подхода, заключающего в том, что требования стандарта могут не учитывать специфики исследуемой информационной системы.

Выработка рекомендаций. Рекомендации, выдаваемые аудитором по результатам анализа состояния информационной системы, определяются используемым подходом, особенностями исследуемой информационной системы, состоянием дел с информационной безопасностью и степенью детализации, используемой при проведении аудита. В любом случае, рекомендации аудитора

должны быть конкретными и применимыми к данной информационной системе, к тому же быть экономически обоснованными, аргументированными (подкрепленными результатами анализа) и отсортированными по степени важности. При этом мероприятия по обеспечению безопасности организационного уровня практически всегда имеют приоритет над конкретными программно-техническими методами защиты [9].

Подготовка отчетных документов. Аудиторский отчет является основным результатом проведения аудита. Его качество характеризует качество работы аудитора. Структура отчета может существенно различаться в зависимости от вида, характера и целей проводимого аудита. По крайней мере должен содержать описание целей проведения аудита; характеристику обследуемой информационной системы; границы проведения аудита; используемые методы; результаты анализа данных аудита; выводы, обобщающие эти результаты и содержащие оценку уровня защищенности информационной системы и/или ее соответствие требованиям стандартов; рекомендации аудитора по устранению существующих недостатков и совершенствованию систем безопасности [9].

Основными видами аудита информационной безопасности, применяемыми на практике, являются [16]:

1. Активный аудит (инструментальный анализ защищенности).
2. Экспертный аудит.
3. Аудит на соответствие стандартам.
4. Дополнительные услуги.

Активный аудит. Один из самых распространенных видов оказываемых услуг. Он включает в себя исследование состояния защищенности информационной системы с позиции злоумышленника: при помощи специального программного обеспечения осуществляется сбор информации о состоянии системы сетевой защиты (те параметры и настройки, на основании использования которых злоумышленник может получить доступ к сети и произвести атаку). Другими словами, перед аудитором ставится задача — смоделировать как можно

больше разнообразных сетевых атак на систему сетевой защиты предприятия имея минимум информации. В результате проведения активного аудита становятся известны все уязвимости, определяются степень их критичности и методы устранения, а также сведения о широкодоступной информации сети заказчика. На основании чего, впоследствии составляются рекомендации по модернизации системы сетевой защиты, которые позволяют устранить выявленные недостатки, повысить уровень защищенности информационной системы от действий злоумышленников и свести к минимуму расходы на обеспечение информационной безопасности [16].

Экспертный аудит. Один из самых объемных видов работ. Он подразумевает сравнение состояния текущего уровня информационной безопасности с требованиями, предъявляемыми руководством компании, к системе информационной безопасности и «идеальной» системой информационной безопасности. В процессе экспертного аудита проводятся следующие виды работ, совместно с представителями компании-заказчика [16]:

- сбор исходных данных об информационной системе: функции, особенности, топология сети, используемые технологии автоматизированной обработки и передачи данных (с учетом планируемых перспектив развития);
- сбор организационно-распорядительных документов по обеспечению информационной безопасности и их анализ (например, политика безопасности, план защиты, различного рода инструкции и приказы);
- выявление точек ответственности систем, устройств и серверов информационной системы;
- составление перечня подсистем всех подразделений компании (с категоризацией критичной информации и схемами информационных потоков) и т. п.

Аудит на соответствие стандартам. При проведении данного вида аудита сравнивается состояние информационной безопасности с описанием, приводимым в стандартах. По результатам проведенного аудита выдается официаль-

ный отчет, в котором прописывается степень соответствия информационной системы компании-заказчика выбранным стандартам и ее внутренним требованиям в области информационной безопасности. Также приводится количество и категории полученных несоответствий и замечаний, даются рекомендации по построению и/или модификации существующей системы информационной безопасности, позволяющие привести ее в соответствие с рассматриваемым стандартом.

Мотивация руководства компаний к прохождению аудита информационной безопасности различна, но в основном сводится к получению сертификата, подтверждающего высокий уровень информационной безопасности в компании, с целью укреплений позиций на рынке для выхода на более крупных клиентов и/или деловых партнеров и расположения их к сотрудничеству [16].

Дополнительные услуги. В ходе проведения аудита заказчику могут предлагается дополнительные услуги, которые напрямую связаны с оценкой состояния системы информационной безопасности, основанные на проведении специализированных исследований с использованием программно-аппаратных средств. Ярким примером является использование компаниями в своей информационной системе специализированного программного обеспечения собственной разработки. Поскольку подобное программное обеспечение является «уникальным», то и как таковых готовых, универсальных или специализированных средств и технологий для их анализа на предмет защищенности и отказоустойчивости не существует. Поэтому в своей работе аудиторы прибегают к использованию: стресс-тестирования и/или теста на проникновение [16].

Стресс-тестирование — исследование производительности и стабильности работы системы, направленное на определение критических точек нагрузки, при которых система в момент атаки перестает адекватно реагировать на легитимные запросы пользователей.

Тест на проникновение или пентест (от англ. Penetration Testing), инструмент анализа защищенности информационной системы основной целью кото-

рого является демонстрация того, к чему удалось получить доступ злоумышленнику, при текущем состоянии системы сетевой защиты.

Также, стоит более детально разобрать понятие «система тестирования» с используемом нами контексте, потому как данное понятие имеет довольно обширное определение. В общем случае, тестирование определяется как процесс, направленный на выявление характеристик информационной системы и демонстрацию различий между ее требуемым и фактическим состоянием (T.Koomen, M.Pol «Test Process Improvement»).

Первоочередными задачами тестирования являются определение соответствия предмета тестирования заданным спецификациям, а также определение пригодности объекта тестирования к выполнению тех или иных функций. В задачи тестирования не входит определение причин несоответствия заданным требованиям. Также, тестирование не обеспечивает само качество, но на его основе формируется представление о степени неопределенности качества системы.

Согласно стандарту ISO 9000 под качеством объекта тестирования понимается совокупность характеристик объекта, относящихся к его способности удовлетворить установленные или предполагаемые требования. Другими словами, чем большему количеству требований соответствует тестируемый объект, тем выше его качество. К тому же тестирование не является отдельной деятельностью или направлением.

Тестирование — один из разделов диагностики и один из инструментов решения проблемы обеспечения качества объекта.

Полный перечень мероприятий по обеспечению качества объекта включает в себя три группы мероприятий [36]:

1. Предупредительные — нацелены на предотвращение дефектов (например: методики, процедуры, шаблоны документов).

2. Выявляющие — нацелены на нахождение недостатков (например, тестирование).

3. Корректирующие — нацелены на устранение недостатков (например, исправление ошибок, найденные в ходе тестирования).

Таким образом, тестирование — это один из способов выявления дефектов. В свою очередь, выявление дефектов — это один из видов деятельности по обеспечению качества объекта. Тестирование определяется по-разному и зависит прежде всего от компании и/или от основных целей его проведения.

1.3 Анализ литературы и интернет-источников

1.3.1 Анализ печатных источников

На начальном этапе работы было проанализировано большое количество информации, представленной, как в Интернете, так и в печатных источниках. После изучения материала, было вынесено заключение о том, что полноценной информации по методике проведения тестирования по оценке рисков и угроз информационной безопасности как для предприятий, так и для образовательных учреждений как таковых не существуют. Имеются отдельные наработки, в плане рассматриваемого теоретического материал по тому, какие угрозы информационной безопасности существуют на настоящий момент, и какие из них наиболее характерны для того или иного типа предприятия, а также описываются объекты, которые в основном подвергаются атакам.

Учебное пособие «Аудит безопасности фирмы: теория и практика» посвящено проблемам аудита информационной безопасности, как одного из направлений деятельности системы безопасности компании [38]. В данном учебном пособии рассматриваются как общие вопросы аудита безопасности компании, так и вопросы аудита отдельных направлений и областей информационной безопасности.

В книге «Аудит информационной безопасности» [7] рассматривается целый комплекс вопросов, связанных с проведением аудита информационной

безопасности на предприятии, даны основные понятия, показана роль анализа и управления информационными рисками. Также, в данной книге проводится описание международных и российских стандартов информационной безопасности, излагаются методологические основы применения стандартов ISO 15408 и ISO 17799 (ныне действующий стандарт ISO 27002-2013) для оценки рисков и управления информационной безопасностью, дана характеристика программных средств, применяемых при аудите информационной безопасности. Автор книги уделяет особое внимание практическим вопросам методики проведения аудита информационной безопасности в компаниях различного типа и уровня.

Виктор Сердюк в своем учебном пособии «Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий» [29] описывает проблемы защиты информационных систем от информационных атак. В основу учебного пособия заложен накопленный многолетний опыт специалистов информационной безопасности по разработке и внедрению комплексных систем безопасности для защиты от информационных атак. Учебное пособие охватывает наиболее значимые и основные темы информационной безопасности, такие как: виды уязвимостей; информационные атаки и их последствия; методика проведения аудита и оценка рисков информационной безопасности; системы обнаружения и предотвращения атак и особенности их практического применения; обучение и сертификация специалистов по информационной безопасности.

Не менее полезным является учебное пособие Юрия Родичева «Нормативная база и стандарты в области информационной безопасности» [28], в котором рассмотрены наиболее важные нормативные документы Федеральной службы по техническому и экспортному контролю (ФСТЭК), а также международные и национальные стандарты Российской Федерации (РФ) в области информационной безопасности, так как на основании рассматриваемой нормативно-правовой базы выстраивается методика проверки предприятия на предмет

соответствия существующей политики информационной безопасности тому или иному закону, стандарту, постановлению и т. п.

1.3.2 Анализ интернет-источников

В статье «Аудит информационной безопасности — основа эффективной защиты предприятия» [10] (рисунок 1), дается определение понятию «аудит информационной безопасности» и приводится подробная характеристика его составляющих, включая основные виды аудита. Также, автор статьи детально описывает основные этапы работ при проведении аудита в компании-заказчике, включая используемые методы и необходимый для проведения аудита перечень исходных данных.

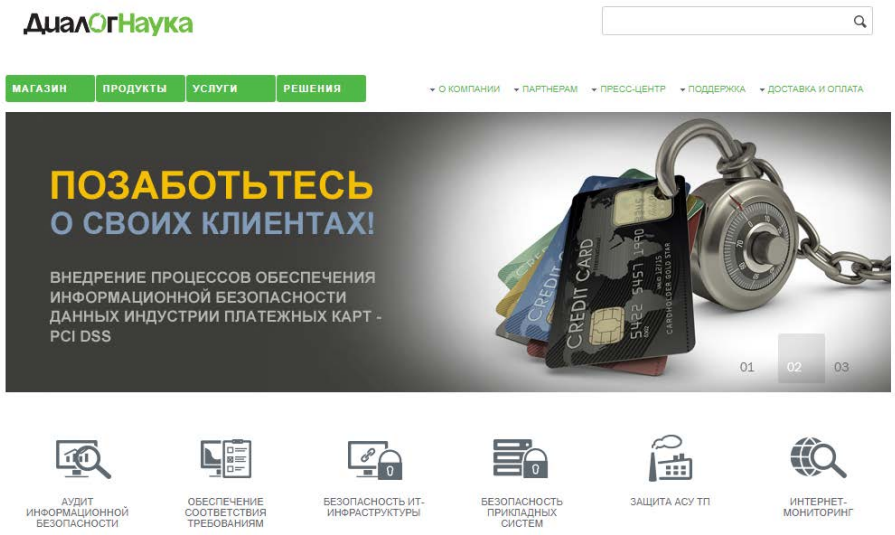


Рисунок 1 — Веб-портал ДиалогНаука

Александр Астахов в своей статье «Аудит безопасности информационных систем» [9] (рисунок 2) рассказывает об обобщенной практике проведения аудита безопасности информационных систем; раскрывает понятие аудита информационной безопасности; обосновывает цели его проведения; рассматривает методы анализа и управления рисками, используемые аудиторами, а также

средства их реализации; действующие стандарты и системы сертификации информационных систем, в рамках которых проводится аудит безопасности.

Также, Александр Астахов является автором другой статьи на смежную тему «Виды аудита информационной безопасности» [9] (рисунок 2), в которой акцентируется внимание на особенности проведения каждого из вида аудита и приводится подробная классификация оказываемых при проведении аудита услуг. Автор приводит критерии оптимального выбора и применения того или иного вида аудита.

Рисунок 2 — Веб-портал ISO 27000 «Искусство управления информационной безопасностью»

В работе кандидата технических наук, эксперта по информационной безопасности, исполнительного директора компании «Digital Security» [30] Ильи Давидовича Медведовского под названием «Практическое применение международного стандарта информационной безопасности ISO 17799» (рисунок 3) содержатся и описываются критерии оценки защищенности информационных систем, критерии проведения аудита безопасности информационных систем, практическое применение международного стандарта ISO 17799 (ныне действующий стандарт ISO 27002-2013) [24]. Данная работа И. Д. Медведовского нашла свою реализацию в программном продукте «Кондор», на основные идеи и принципы функционирования которого мы опирались при создании и разработке программного продукта.

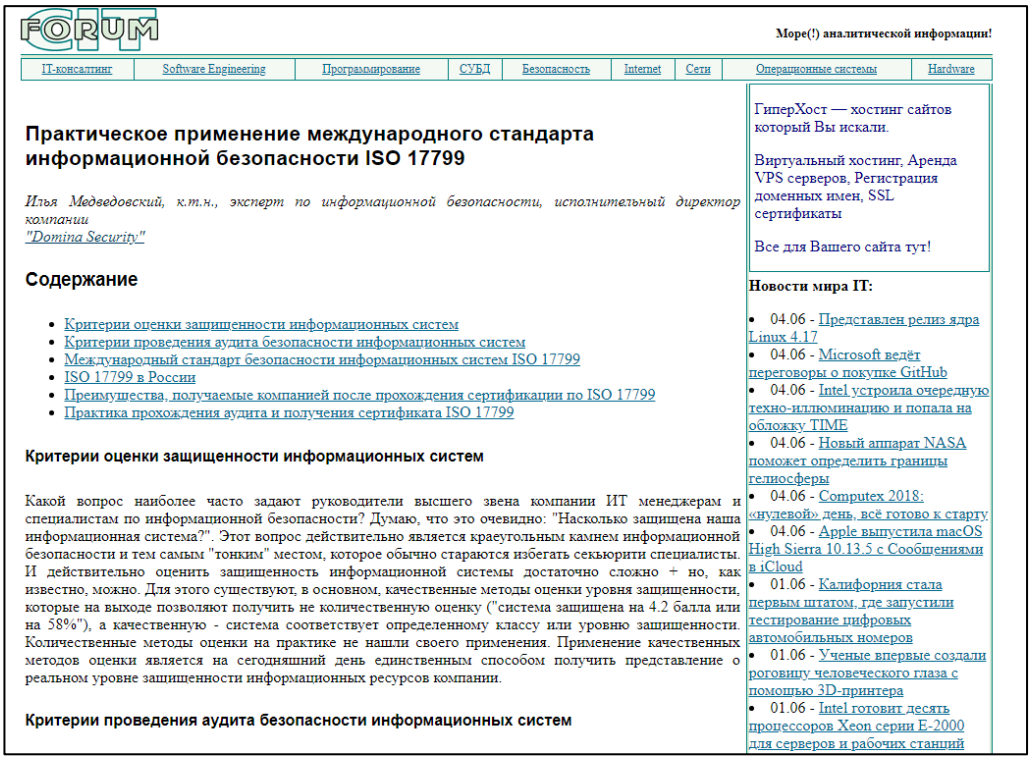


Рисунок 3 — Веб-портал CitForum

В своей работе «Стандарт на страже информационной безопасности» [35] (рисунок 4) эксперт информационной безопасности С. И. Игнатенко заявляет и раскрывает важность использования и практическую пользу от применения международных стандартов в сфере информационной безопасности, в частности международного стандарта ISO 17799 (ныне действующий стандарт ISO 27002-2013). Эксперт говорит о том, что «в связи с ростом зависимости организаций от информационных систем и сервисов происходит резкое увеличение рисков, связанных с недостаточным уровнем обеспечения безопасности получения, хранения и переработки информации. Сложность информационных систем и необходимость их интеграции в общедоступные приводит к невозможности или значительному затруднению осуществления контроля над обеспечением безопасности информации и ресурсов. Возникает острая необходимость в стандартизации систем и процессов информационной безопасности» [35].

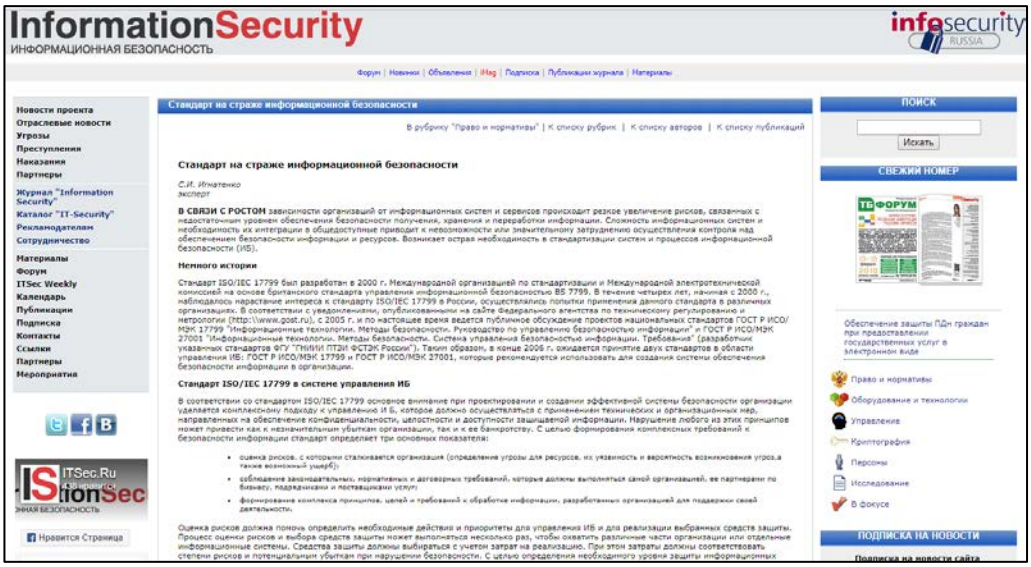


Рисунок 4 — Веб-портал InformationSecurity

1.3.3 Анализ аналогичных систем и тестов

Как таковых современных аналогов разработанному программному продукту по выбранным международным стандартам ISO 27002 и ISO 15408 в открытых источниках сети Интернет нам найти не удалось.

Хочется отметить, что основная идея в разработке системы тестирования по современным международным стандартам в области информационной безопасности как таковой была взята с опорой на принцип реализации и функционирования программного продукта «Кондор», который является коммерческим проектом компании DigitalSecurity [30]. Программный продукт «Кондор» (функционирует в связке с программным продуктом «Гриф», устанавливаемые одним пакетом) — система разработки и управления политикой информационной безопасности компании на основе международного стандарта ISO 17799 [33], предназначенная для разработки положений политики информационной безопасности компании и управления процессом внедрения их на практике. Данный проект был закрыт по инициативе руководства самой компании в 2008 году, вместе с его распространением, поддержкой и обслуживанием. Компания изменил вектор своей коммерческой деятельности.

На практике аудиторы, занятые в сфере информационной безопасности, при проведении проверок пользуются несколькими программными продуктами.

Данные программные продукты имеют нечто схожее с принципами функционирования разработанной нами системы тестирования, поскольку в основу их работы также заложены тестовые вопросы, но их спецификация отлична от той, которая была предложена нами. Примеры программных продуктов, имеющие максимально близкий функционал:

1. Программное обеспечение RiskWatch, разрабатываемое одноименной американской компанией, является довольно мощным инструментом анализа и управления рисками, по сравнению со своими конкурентами. Также, этим его отличает крайне высокая стоимость. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности и анализа рисков [25]:

- RiskWatch for Physical Security — служит для оценки физических методов защиты информационной системы;
- RiskWatch for Information Systems — разработано для оценки информационных рисков;
- RiskWatch RW17799 for ISO17799 — используется для оценки требованиям стандарта ISO17799 (ныне действующий стандарт ISO 27002-2013).

2. Система COBRA, разрабатываемая австралийской компанией Risk Associates — инструмент для анализа рисков и оценки соответствия информационной системы стандарту ISO 17799 (современный аналог ISO 27002-2013). COBRA реализует методы количественной оценки рисков, а также инструменты для консалтинга и проведения обзоров безопасности. При разработке инструментария COBRA были использованы принципы построения экспертных систем, обширная база знаний по угрозам и уязвимостям, а также большое количество вопросников, с успехом применяемые на практике [26].

1.4 Анализ международных стандартов информационной безопасности

Современному специалисту информационной безопасности без знаний соответствующих стандартов и законодательства в области информационной безопасности попросту не обойтись. Самая главная причина заключается в том, что ими регулируются основные направления деятельности, виды и формы работ, направленные на обеспечение информационной безопасности, а также определяется необходимость четкого следования им, поскольку они составляются и постоянно обновляются на фоне собираемого мирового опыта.

Международный стандарт ISO/IEC 15408 был разработан на основе стандарта «Общие критерии безопасности информационных технологий». Современный аналог данного стандарта в РФ носит название ГОСТ Р ИСО/МЭК 15408 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» [17,18,19] и состоит из трех частей:

1. Введение и общая модель [17].
2. Функциональные компоненты безопасности [18].
3. Компоненты доверия к безопасности [19].

Хочется отметить, что ранее в отечественных нормативных документах в области информационной безопасности, до выхода данного стандарта, понятие риска не вводилось. Стандарт разработан таким образом, чтобы удовлетворить потребности трех групп специалистов: разработчиков, экспертов по сертификации и пользователей объекта оценки. Под объектом оценки понимается подлежащий оценке продукт информационных технологий или система с руководствами администратора и пользователя. К таким объектам относятся: операционные системы, прикладные программы, информационные системы и т. д. Стандарт предусматривают наличие двух типов требований безопасности:

1. Функциональные требования безопасности, которые относятся к сервисам безопасности: идентификация, аутентификация, управление доступом, аудит и т. д.

2. Требования доверия к безопасности, которые относятся к технологии разработки, тестирования, анализа уязвимостей, поставке, сопровождения и т. д.

Чтобы структурировать пространство требований, в стандарте используется иерархия «класс-семейство-компонент-элемент»: классы определяют наиболее общую, «предметную» группировку требований; семейства в пределах класса различаются по строгости и другим нюансам требований; компонент — минимальный набор требований, фигурирующий как целое; элемент — неделимое требование [23,32].

В стандарте выделены 11 классов функциональных требований:

- аудит безопасности;
- связь (передача данных);
- криптографическая поддержка (криптографическая защита);
- защита данных пользователя;
- идентификация и аутентификация;
- управление безопасностью;
- приватность (конфиденциальность);
- защита функций безопасности объекта;
- использование ресурсов;
- доступ к объекту оценки;
- доверенный маршрут/канал.

Международные стандарты ISO/IEC 17799, ISO/IEC 27001, ISO/IEC 27002 взаимосвязаны друг с другом, потому как посвящены вопросам управления (менеджменту) информационной безопасностью.

Международный стандарт ISO/IEC 27001 «Информационные технологии — Технологии безопасности — Системы менеджмента информационной безопасности — Требования» [34] (от англ. «Information technology — Security techniques — Information security management systems — Requirements») был разработан в 2005 году на основе стандарта BS 7779-2:2002 (рисунок 5). В стандарте ISO 27001 аккумулированы описания лучших мировых практик в области управления информационной безопасностью. В нем также устанавливаются требования к системе менеджмента информационной безопасности предприятия, с целью установления способности предприятия защищать свои информационные ресурсы. Международный стандарт ISO 27001 подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности, основной целью которой является выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон. В Российской Федерации современный аналог стандарта ISO/IEC 27001 носит название ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [20].

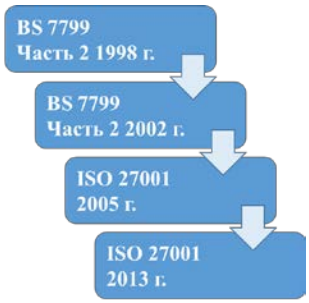


Рисунок 5 — Этапы развития стандарта ISO/IEC 27001:2013

Международный стандарт ISO/IEC 27002 «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности» (от англ. Information technology — Security techniques — Code of practice for information security management) был разрабо-

тан (рисунок 6) в 2005 году на основе стандарта ISO 17799, который был опубликован в 2000 году и является полной копией Британского стандарта BS 7799-1:1999 «Практические правила управления информационной безопасностью» (от англ. Code of Practice for Information Security Management). Стандарт BS 7799-1:1999 описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации и служит практическим руководством по созданию СУИБ, хоть и изначально предназначался для определения норм безопасности при ведении коммерческой деятельности [31]. Стандарт ISO/IEC 27002 содержит лучшие практические советы и рекомендации по разработке и внедрению компаниями системы менеджмента информационной безопасности, в контексте выбора, внедрения и использования средств управления имеющимися рисками. Он содержит более полное описание и рекомендации по внедрению средств управления информационной безопасностью по сравнению с международным стандартом ISO/IEC 27001:2013. В Российской Федерации современный аналог стандарта ISO/IEC 27002 носит название ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [21].

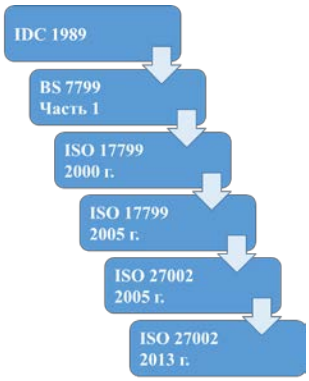


Рисунок 6 — Этапы развития стандарта ISO/IEC 27002:2013

На основании изученной информации можно сделать вывод о том, что актуальность в разработке программного продукта существует, поскольку были наработки по устаревшим стандартам, в то время как по актуальным стандар-

там подобных систем найти не удалось. На сегодняшний день оценка рисков информационной безопасности на предприятиях производится на основании международного стандарта ISO/IEC 27002, знание которого необходимо для современного специалиста по информационной безопасности. С практической точки зрения стандартов и спецификаций (международные, национальные и т. п.) в области информационной безопасности очень и очень много, но каждый уважающий себя специалист должен обладать знаниями и иметь представления о наиболее популярных стандартах: ISO 15408, ISO 27001, ISO 27002 (бывший ISO 17799).

2 ОПИСАНИЕ СИСТЕМЫ ТЕСТИРОВАНИЯ

2.1 Назначение продукта

Разработанный нами программный продукт нацелен на использование его возможностей как коммерческими предприятиями, так и образовательными организациями, с целью проверки текущего состояния информационной безопасности компании на предмет выявления существующих уязвимостей и оценку рисков угроз информационной безопасности.

Принцип работы программного продукта имитирует процедуру проверки рисков и уязвимостей в компании, подобно той, которую применяют аудиторы, используя свои собственные методы и программные средства. Отличие заключается лишь в том, что при проведении процедуры аудита аудиторы запрашивают у руководства компании необходимую информацию, проверяя ее и требуемые стандартами критерии в компании-заказчике, редко ссылаясь на подробности проводимой ими проверки, а выдавая лишь на конечном этапе информацию о найденных уязвимостях, нарушениях и способах их устранения. Так на основании полученной информации, сформированной по результатам прохождения тестирования, руководством компании самостоятельно могут быть предприняты дополнительные меры по оценке или совершенствованию существующей системы информационной безопасности: совершенствование политики безопасности, формирование определенных инструкций и правил для персонала внутри организации, либо для самостоятельной подготовки к аудиту, поскольку продукт основан на используемых аудиторами международных стандартах в области информационной безопасности: ISO/IEC 27002, ISO/IEC 15408 и проверяет часть предъявляемых стандартами и проверяемых аудиторами требований, и критериев в компании.

Система тестирования представляет собой ничто иное как веб-приложение с подключенными к нему: плагином тестирования и банком вопросов. При прохождении тестирования плагин собирает полученные ответы на входе, а затем выводит по ним статистику, в которой отражается результат пройденного тестирования — сумма набранных баллов. В отчете по пройденному тестированию будет подробно выведена информация, при ответе на какой вопрос было допущено нарушение одного или нескольких требований и/или рекомендаций международных стандартов в области информационной безопасности.

В силу своей особенности данный программный продукт будет интересен:

- студентам, обучающимся по направлению подготовки и преподавателям, ведущим дисциплины в рамках данных направлений подготовки: 44.03.04 Профессиональное обучение (по отраслям), профиль подготовки «Информатика и вычислительная техника», профилизация «Информационная безопасность»; 10.03.01 Информационная безопасность; 38.04.09 Государственный аудит и т. п.;
- руководителям коммерческих предприятий или образовательных организаций, а также лицам ответственным за информационную безопасность в компании;
- специалистам и аудиторам, занятым в области информационной безопасности.

2.2 Описание банка вопросов

Для планируемой системы тестирования по стандарту ISO 27002 (бывший стандарт ISO/IEC 17799) был разработан банк вопросов, который включает в себя 325 вопросов, разделенные на 10 разделов (Таблица 1).

Банк вопросов состоит из вопросов закрытой формы с выбором одного варианта ответа по принципу противоположности (Приложение Б).

Таблица 1 — Содержание банка вопросов

Раздел	Характеристика раздела	Объем
Политика безопасности	Данный раздел содержит вопросы о существующей организации политики безопасности: положения политики, порядок внесения изменений, утверждения политики.	14
Организация информационной безопасности	Данный раздел содержит вопросы о принятых в компании организационных мерах по обеспечению информационной безопасности и об ответственности за ее обеспечение	16
Управление ресурсами	Данный раздел содержит вопросы о процедуре учета ресурсов и о классификации и категоризации информации.	10
Безопасность персонала	Данный раздел содержит вопросы о процедуре приема сотрудников на работу, об уровне осведомленности персонала по вопросам информационной безопасности и о действиях, осуществляемых персоналом в случае инцидентов в области информационное безопасности.	16
Физическая безопасность и безопасность окружения	Данный раздел содержит вопросы о физическом контроле доступа к ресурсам, содержащим ценную информацию, и о физических угрозах оборудованию.	39
Управление коммуникациями и операциями	Данный раздел содержит вопросы о процедурах внесения изменений в среду выполнения бизнес-операций, об антивирусной защите, о контроле целостности, резервном копировании информации и восстановлении из резервных копий, о правилах обращении с информацией и программным обеспечением при передаче, о безопасности электронной коммерции и электронного офиса. Вопросы раздела отражают процесс безопасной обработки передачи информации.	73
Управление доступом	Данный раздел содержит вопросы о правах и привилегиях пользователей при доступе к ресурсам организации, о политике сетевых служб, о парольной политике, о мониторинге процедур повышенного риска, о доступе мобильных и удаленных пользователей к ресурсам организации. Вопросы раздела отражают распределение доступа к ценным ресурсам организации.	66
Приобретение, разработка и поддержка систем	Данный раздел содержит вопросы о проверках входных и выходных данный систем, о системе криптографической защиты информации, о правилах внесения изменений в исполняемые файлы и библиотеки, о правилах работы с тестовой средой, о приобретении программных продуктов.	42
Управление бесперебойной работой организации	Данный раздел содержит вопросы о планах обеспечения непрерывности ведения бизнеса, о восстановлении системы после сбоев, о тренингах персонала по действиям в случае аварийных ситуаций.	24
Соответствие	Данный раздел содержит вопросы о лицензионных соглашениях	25

нормативным требованиям	приобретенного программного обеспечения, о соответствии системы стандартам информационной безопасности, о критериях сохранения улик, о проверках, проводимых в информационной системе: например, проверка технического соответствия, сторонний аудит.	

Разработанные вопросы отвечают требованиям, предъявляемым:

1. К формулировке тестовых заданий в закрытой форме с выбором одного правильного ответа по принципу противоположности.
2. Международными стандартами на предмет:
   - соответствия изложенного в них материала;
   - правдоподобности и правильности формулировки вопросов к проверяемым стандартами требований, правил и норм;
   - полноты оценки состояния текущего уровня информационной безопасности на предприятии, проверяемых параметров и степени их соответствия международным стандартам.

2.3 Выбор средства реализации

Перед тем, как приступить к непосредственной разработке программного продукта, перед нами встал выбор средства реализации, в котором можно было бы начать разработку задуманной идеи. Перед нами был выбор использования следующих сред для разработки программного продукта:

1. **Joomla** — система управления содержимым (**CMS**) с открытым исходным кодом, разработанная на языках **PHP** (от англ. Hypertext Preprocessor — скриптовый язык общего назначения) и **JavaScript** (объектно-ориентированный язык программирования, используемый для добавления форм интерактивности для веб-сайта) и использующая в качестве хранилища базы данных систему управления базами данных (СУБД) **MySQL** [4]**.**
2. **WordPress** — система управления содержимым сайта с открытым исходным кодом, написанная на языке **PHP**, с реализованным сервером базы данных в СУБД **MySQL** [6].

3. **Drupal** — система управления содержимым, используемая как каркас для веб-приложений (**CMF**), написанная на языке PHP и использующая в качестве хранилища реляционную базу данных (поддерживаются MySQL, PostgreSQL и др.). Особо хочется отметить, что Drupal является свободным программным обеспечением и развивается усилиями людей со всего мира [3].

4. **«Ручная верстка»**. Поскольку учебный план по нашему профилю подготовки не предполагает углубленного изучения языков и сред программирования, мы решили отказаться от идеи написания сайта и плагина «вручную».

Сопоставив все достоинства и недостатки Joomla, WordPress и Drupal, мы выбрали в качестве среды разработки CMS **Joomla** версии **2.5.17** (рисунок 7) по следующим значимым причинам, которые были определены, как наиболее значимые и пригодные для дальнейшей работы:

- простота использования, нетребовательность к временным затратам на понимание структуры и конструирование сложных сайтов;
- большое количество готовых разработанных шаблонов и модулей;
- изначальная ориентированность на электронную коммерцию и социальные площадки;
- удобство внесения правок как в программном коде, так и в самой структуре сайта;
- улучшенная подготовленность к монетизации сайта и возможность продвинутой настройки продвижения сайта в поисковых системах (SEO);
- система более надежна, за счет постоянно разрабатываемых обновлений, выявления и устранения уязвимостей и повышении уровня безопасности.

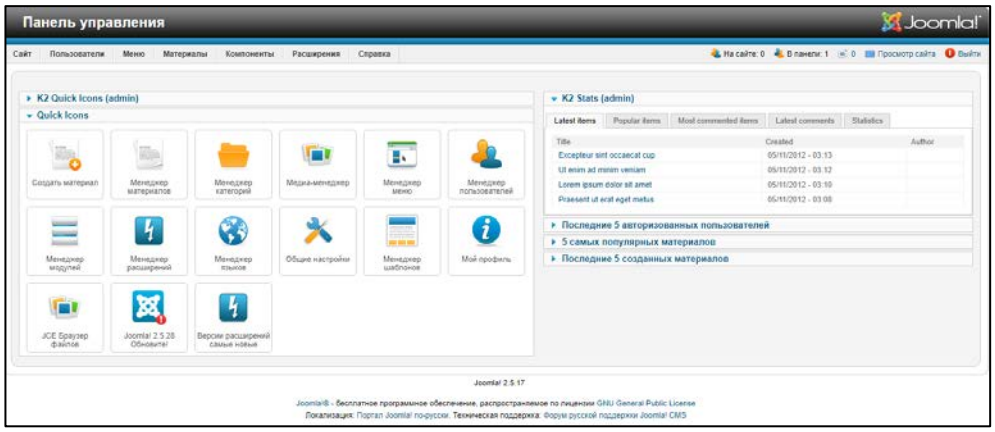


Рисунок 7 — Панель управления CMS Joomla версии 2.5.17

Определившись с выбором среды разработки, мы начали поиск плагинов для проведения системы тестирования. Выбор был между двумя максимально подходящими продуктами:

- **Joomla! Quiz Deluxe** — выпущенный компанией Joomla компонент для создания и проведения тестов, онлайн-опросов любой сложности и разнообразной логикой подсчета результатов. Лицензионная платная версия продукта дает возможность использовать любой из 17 типов предлагаемых типов вопросов, а также производить гибкую настройку тестов в соответствии с предъявляемыми требованиями [5].
- **ARI Quiz Lite** — русифицированный бесплатный конструктор форм тестов для проверки уровня знаний посетителей сайта с открытым кодом. Его основные возможности и преимущества: управление доступом пользователей к тестам, подробная статистика результатов тестирования, групповое тестирование по категориям, использование шаблонов при построении тестов и вопросов к нему [2].

По итогу был выбран плагин — **ARI Quiz Lite** (рисунок 19). Это обусловлено сразу несколькими причинами: во-первых, он является наиболее универсальным средством для проведения тестирования и распространяется абсолютно бесплатно; во-вторых, в него интегрирована поддержка русского языка, вследствие чего русифицировано управление; в-третьих, он обладает всеми не-

обходимыми функциями, а также поддерживает возможность внесения каких-либо сторонних изменений со стороны пользователя, исходя их его потребностей. Выбранный плагин впоследствии был доработан в соответствии с задачами выпускной квалификационной работы и идеи работы программного продукта в целом, в котором определяются и задаются определенные параметры для оценки.

2.4 Описание шаблона и структура меню

При разработке оболочки нами был использован готовый шаблон, который был подключен, видоизменен, доработан и наполнен содержимым исходя из задуманных идей и задач выпускной квалификационной работы.

Готовая версия программного продукта содержит обзорный теоретический материал по теме выпускной квалификационной работе в соответствии с определенными разделами (рисунок 10) и предполагает возможность прохождения тестирования исходя из статуса пользователя:

1. **Гость**. В статусе «Гость» пользователю будет доступен лишь ограниченный функционал программного продукта. Он сможет изучать теоретический материал и ознакомиться с основной идеей разработанной системы тестирования, ответив на предлагаемые демо-версией программного продукта вопросы в разделе *Тестирование→Демо-версия*.
2. **Зарегистрированный пользователь**. Пройдя процедуру регистрации (рисунок 8, 9) пользователю станут доступны дополнительные возможности программного продукта, поскольку теперь он сможет выбирать между тем, пройти ли ему тестирование целиком или проверить какую-либо одну категорию, причем количество попыток прохождения не ограничены.

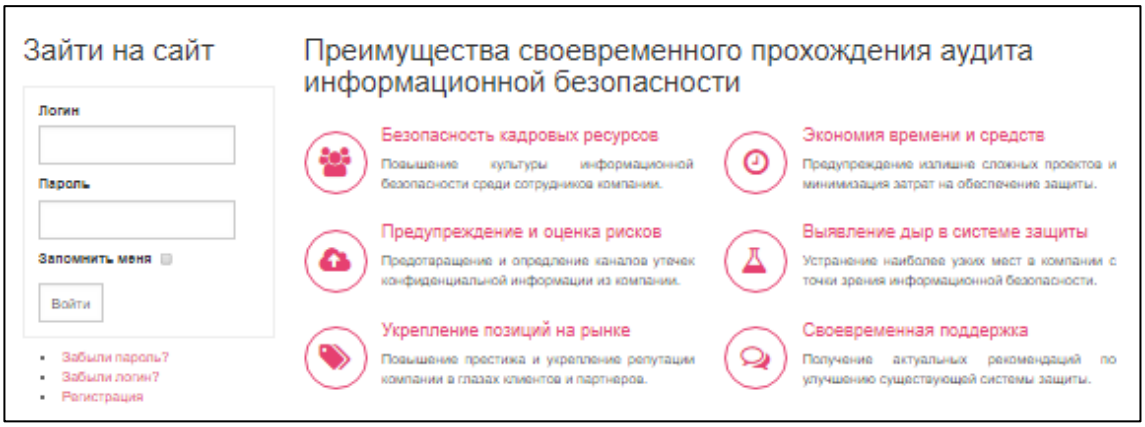


Рисунок 8 — Форма входа, регистрации и восстановления данных пользователей

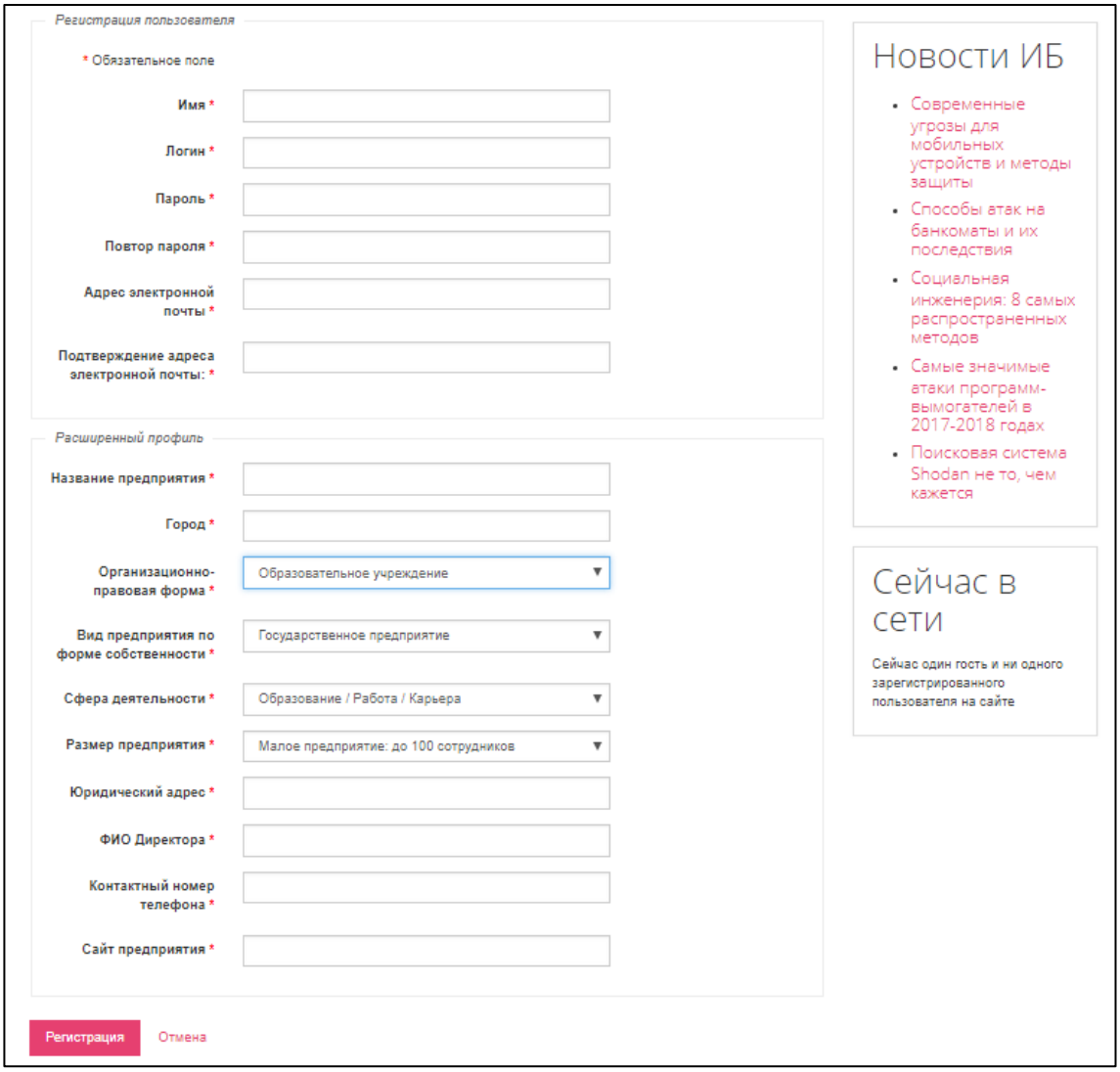


Рисунок 9 — Форма прохождения регистрации пользователей

Пункты управляющего меню в готовой версии программного продукта определены в шесть отдельных групп, некоторые из которых имеют подкатегории (рисунок 10):

1. **Главная**. Данная страница содержит описание процедуры аудита информационной безопасности, определяет и подчеркивает важность его своевременного прохождения и демонстрирует предприятия, которые уже прошли данную процедуру и остались довольны результатом (рисунок 11).

2. **О проекте**. На данной странице представлено непосредственное описание самой идеи проекта: его цель, возможности и предназначение (рисунок 12).

3. **Аудит ИБ**. Содержит информацию об аудите информационной безопасности, в которой дается его определение, характеризуются его виды, описываются этапы проведения и т. д. (рисунок 13).

4. **Тестирование**. В данном разделе дается определение и характеризуется специфика тестирования информационных систем и политик безопасности на предмет соответствия требованиям и рекомендациям международных и национальных стандартов РФ в области информационной безопасности. Также, в данном разделе расположены управляющие кнопки для выбора и перехода к интересующему тесту, в том числе и к тестированию по отдельным категориям.

5. **Стандарты и ГОСТ**. В данном разделе аккумулированы действующие международные стандарты и ГОСТ РФ, на которые мы опирались при разработке программного продукта и которые регулируют деятельность в области информационной безопасности (рисунок 14, 15, 16).

6. **Разработчики**. Данный раздел рассказывает об авторах и разработчиках программного продукта (рисунок 17).

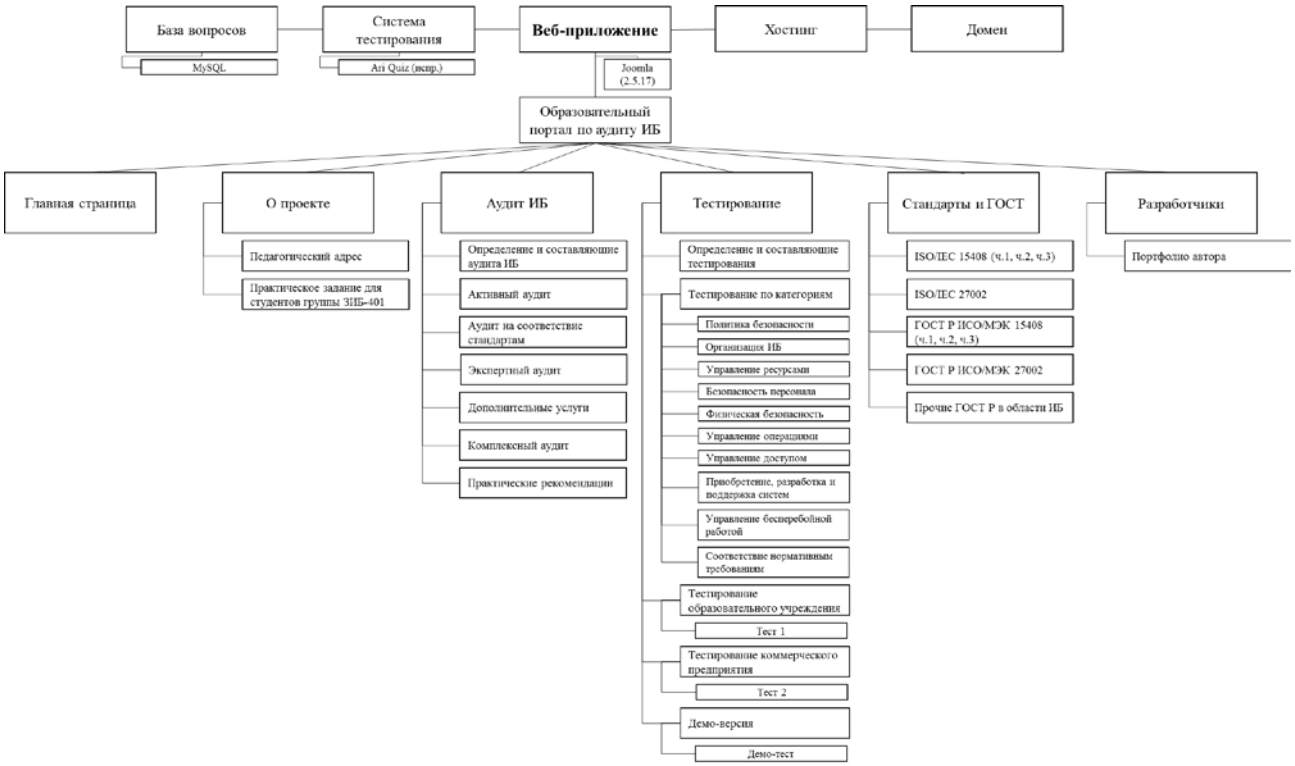


Рисунок 10 — Структура программного продукта

Также стоит отметить, что помимо версии для персональных компьютеров, был разработан и оптимизирован шаблон отображения программного продукта для планшетных устройств.

2.5 Описание интернет-сайта

Разработанный программный продукт с включенной в него системой тестирования представляет собой веб-приложение (иначе говоря сайт), размещеннлн на своем домене и отдельном хостинге, что обеспечивает круглосуточный и постоянный доступ к нему.

При разработке интерфейса программного продукта было реализовано внушительное количество модулей и средств интерактивности. В основном они расположены на главной странице, с целью повышения восприятия информации, упрощения переходов к нужному разделу, получения эффекта интерактив-

ности в веб-приложении. Рассмотрим, как некоторые общие, так и содержащиеся на странице «**Главная**» (рисунок 11) модули веб-приложения:

- «**Управляющие меню (панель управления)**» (общий). Представляет собой навигационную панель, на которой размещены основные пункты меню с переходами в категории и подкатегории. Здесь расположена основная содержательная часть программного продукта;
- «**Слайдер (топ-меню)**». Данный модуль представляет собой автоматически пролистываемую презентацию, состоящую из изображений, на которых приводится описание идеи программного продукта, его преимущества и возможности;
- «**Зайти на сайт**». В этом модуле реализована возможность регистрации пользователей, прохождения ими авторизации (после которой для них становятся доступны дополнительные функции), восстановление забытого пользователем логина или пароля;
- «**Преимущества своевременного прохождения аудита информационной безопасности**». В содержании данного модуля вынесены и раскрыты ключевые преимущества прохождения аудита информационной безопасности;
- «**Оценить угрозы и риски Вашего предприятия**». Данный модуль содержит описание возможностей программного продукта и позволяет через кнопку «Пройти тестирование» перейти к разделу «Тестирование по категориям»;
- «**Аудит ИБ**». В данном модуле приводится определение понятия — аудит информационной безопасности;
- «**Виды аудита информационной безопасности**». Данный модуль представляет собой слайдер, в котором собраны основные виды аудита информационной безопасности, проводимые на предприятиях. Каждая форма, представляет собой управляемую кнопку, которая при нажатии на нее, переводит на страницу с содержанием описания определенного вида аудита.

- «**Новости**» (рисунок 11) и «**Новости ИБ**» (рисунок 12). Эти два модуля представляют собой ничто иное как автоматически конфигурируемые RSS-ленты с содержанием статей, новостей и обзоров из мира информационной безопасности, публикуемые на информационном портале Anti-Malware [1];
- «**Нам доверяют и уже прошли тестирование**». В данном модуле, выносятся логотипы тех предприятий, которые прошли тестирование через веб-приложение;
- «**Календарь**» и «**Сейчас в сети**» (общие). Представляют собой отдельные подключаемые модули, размещаемые на каждой активной странице, которые информируют пользователей веб-приложения о текущей дате и количество посетителей, находящихся на сайте в данный момент (рисунок 12).

Рисунок 11 — Разработанное веб-приложение. Страница «Главная»

Страница «**О проекте**» (рисунок 12) содержит описание общего назначения продукта, его основной идеи и возможностей. Также, описывается потенциальная аудитория и требования к использованию.

В пункте меню «**Аудит ИБ**» (рисунок 13) собран теоретический материал об аудите информационной безопасности в целом: приводится определение понятию «аудит информационной безопасности»; приводится описание, характеристика и виды проводимых работ по тому или иному виду или же этапу проведения аудита; даются некоторые практические рекомендации, как обезопасить предприятие от угроз.

Рисунок 12 — Разработанное веб-приложение. Страница «О проекте»

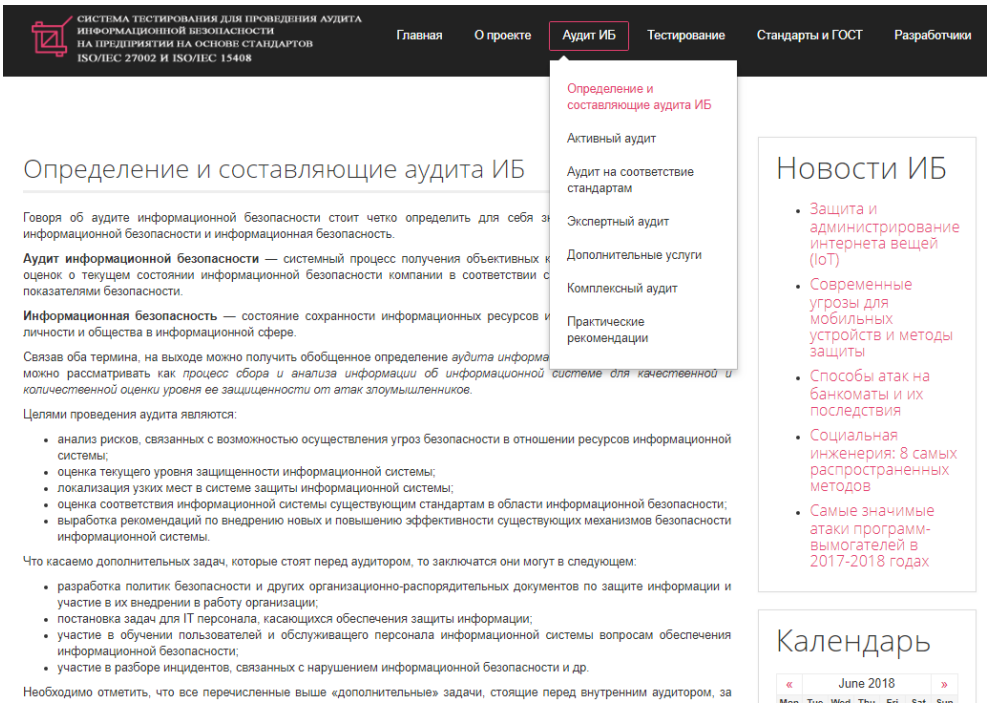


Рисунок 13 — Разработанное веб-приложение. Страница «Аудит ИБ»

Пункт меню «**Стандарты и ГОСТ**» (рисунок 14) содержит ссылки для перехода к PDF-версии (рисунок 15) конкретного международного стандарта или национального стандарта РФ, регулирующего деятельность в области информационной безопасности, которая открывается в новом окне браузера.

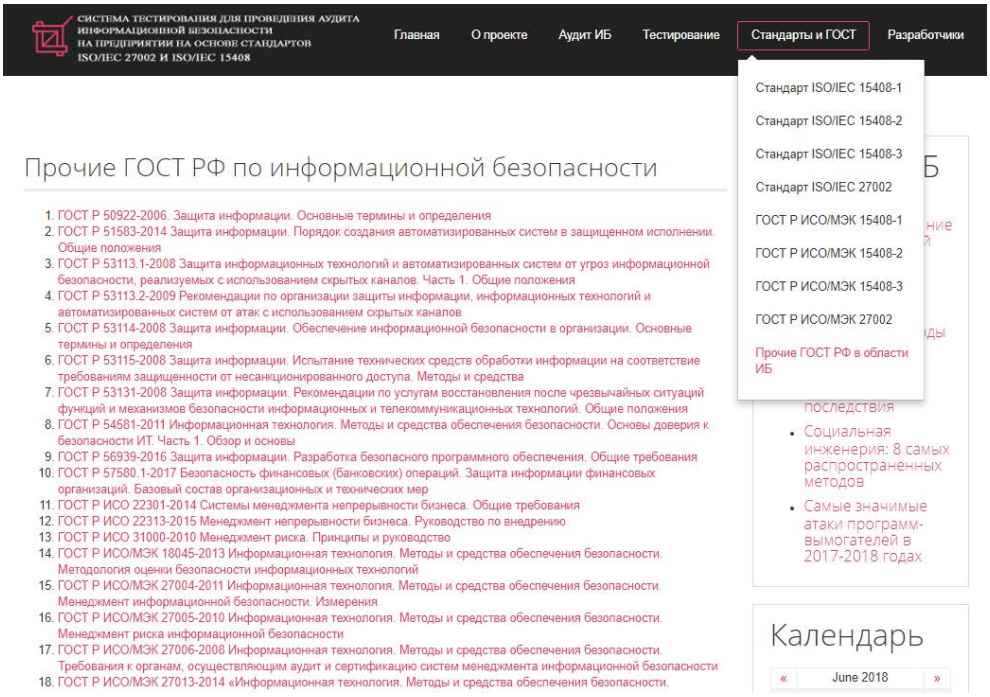


Рисунок 14 — Разработанное веб-приложение. Страница «Стандарты и ГОСТ»

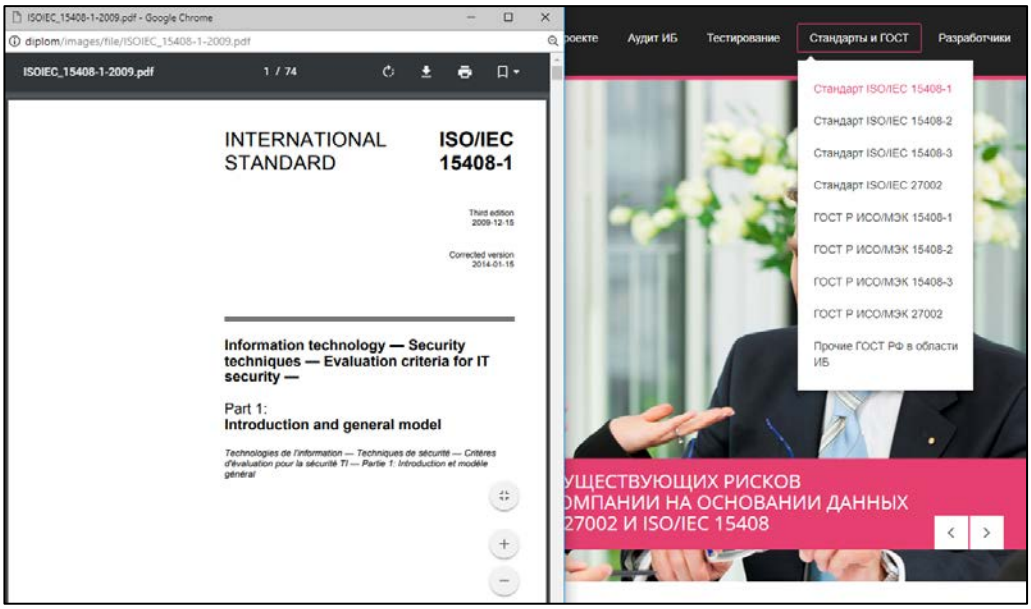


Рисунок 15 — PDF-версия стандарта, отрытого в новом окне по ссылке из пункта меню

В пункте меню «**Тестирование**» на странице «Определение и составляющие тестирования» (рисунок 16) приводится небольшой теоретический материал, в котором раскрывается определение и содержание тестирования информационных систем на предмет оценки рисков. Также, в данном пункте меню собраны основные доступные для прохождения категории и виды тестов.

Страница «**Разработчики**» (рисунок 17) содержит информацию о разработчиках программного продукта.

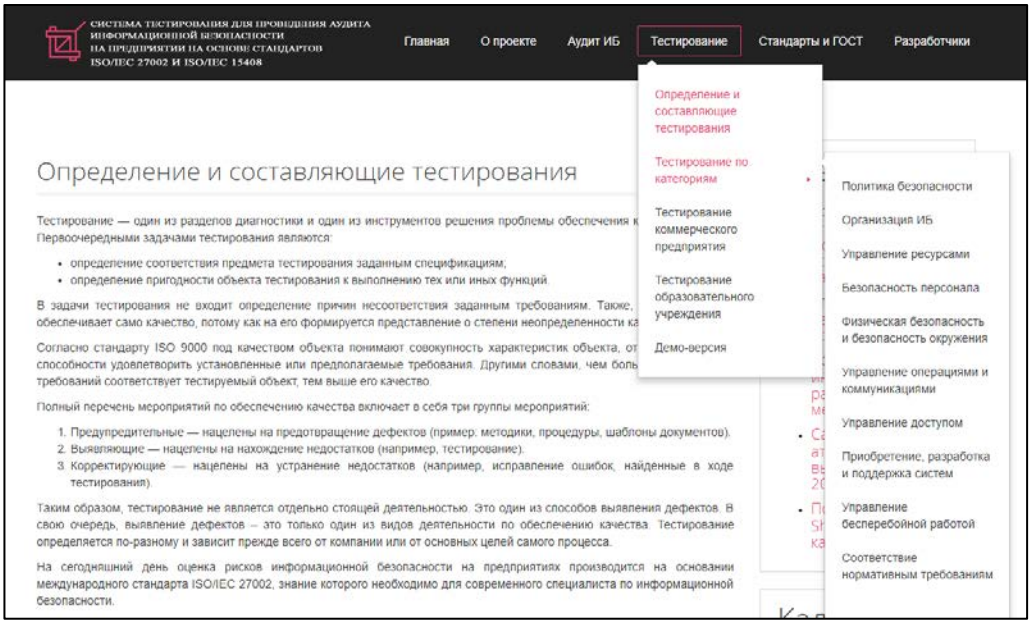


Рисунок 16 — Разработанное веб-приложение. Страница «Тестирование»

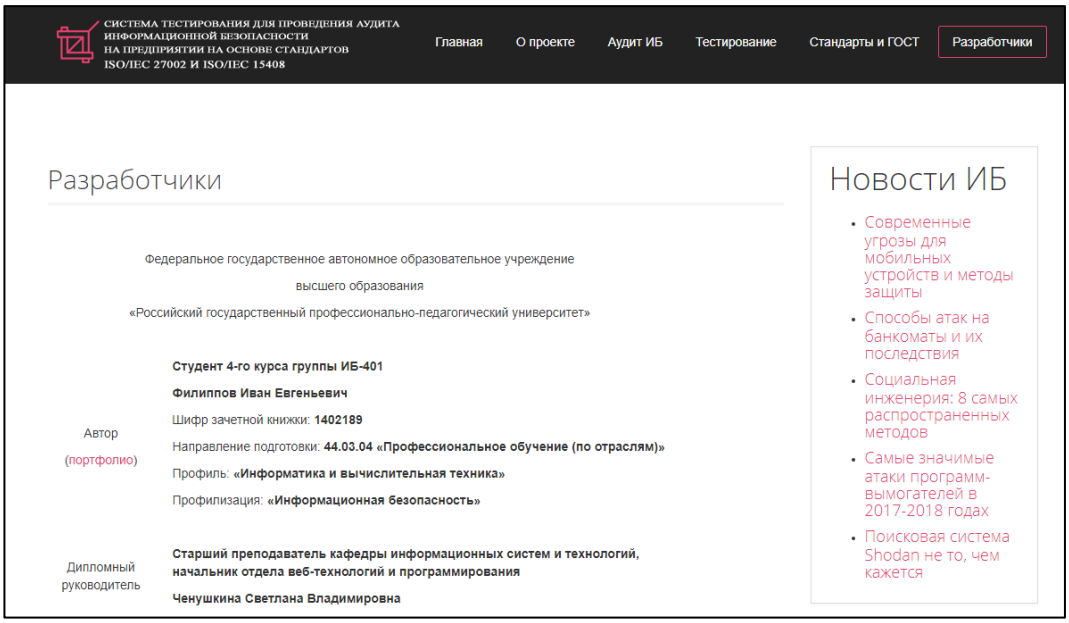


Рисунок 17 — Разработанное веб-приложение. Страница «Разработчики»

Внизу веб-приложения была сформирована отдельная, так называемая «нижняя панель» (рисунок 18), в которую были вынесены следующие модули:

- «**О нас**». Данный модуль содержит рассказ об авторах-разработчиках программного продукта и по управляющей кнопке «Подробнее» переводит пользователя на страницу «Разработчики» (рисунок 17);
- «**Связаться с нами**». В материалах этого модуля размещены контакты для связи с авторами-разработчиками программного продукта;
- «**Полезные ссылки**». В этом модуле аккумулированы активные ссылки для перехода к ознакомлению с содержанием конкретных международных и национальных стандартов РФ в области информационной безопасности, которые были задействованы при разработке программного продукта. Активные ссылки данного модуля равноценны ссылкам, собранным во вкладке «Стандарты и ГОСТ» управляющего меню, отличие заключается лишь в том, что перед ссылкой на PDF-версию документа приведено небольшое описание того или иного стандарта.

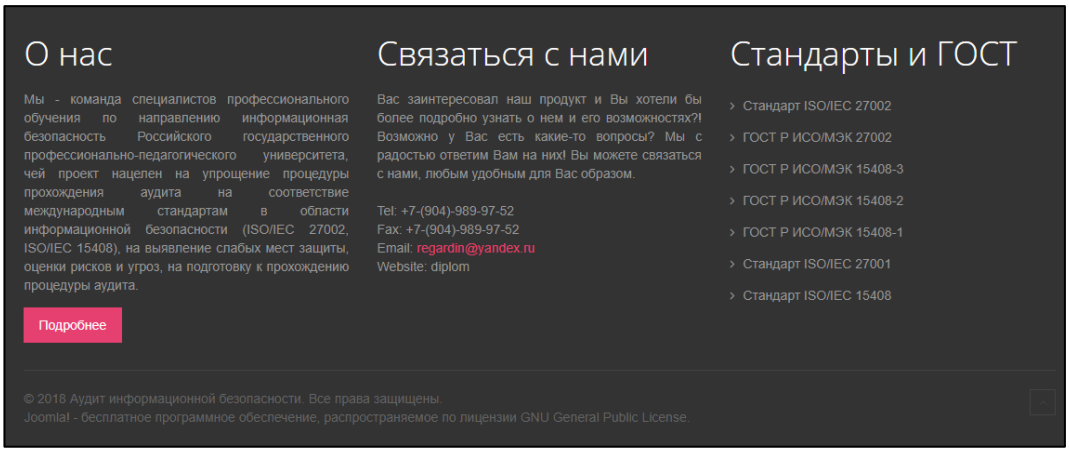


Рисунок 18 — Разработанное веб-приложение. Нижняя панель

2.6 Описание плагина тестирования

К разработанному веб-приложению была подключена система тестирования (рисунок 19, 20, 21, 22, 23, 24), которая как таковая представляет собой отдельный, доработанный, подключаемый к Joomla плагин — **ARI Quiz** [2], основные задачи которого заключаются в аккумулировании и проверке полученных от тестируемых ответов, с возможностью дальнейшей отправки результатов тестирования по указанного пользователем при регистрации e-mail.

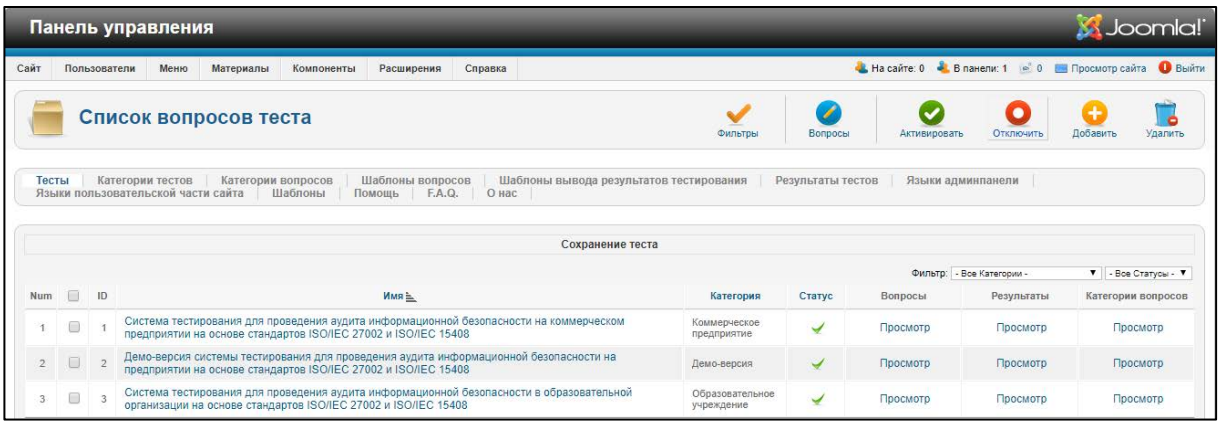


Рисунок 19 — Плагин тестирования. Разработанные виды тестов

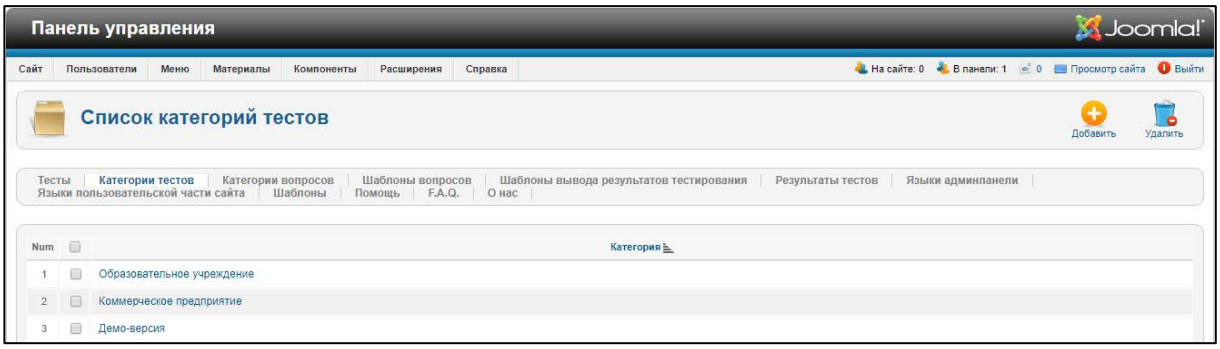


Рисунок 20 — Плагин тестирования. Разработанные категории тестов

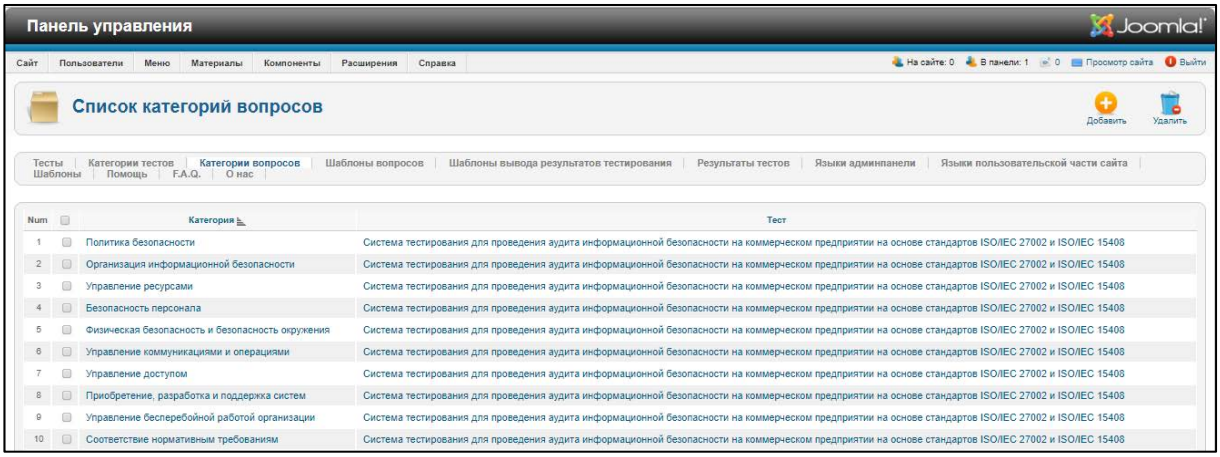


Рисунок 21 — Плагин тестирования. Разработанные категории вопросов

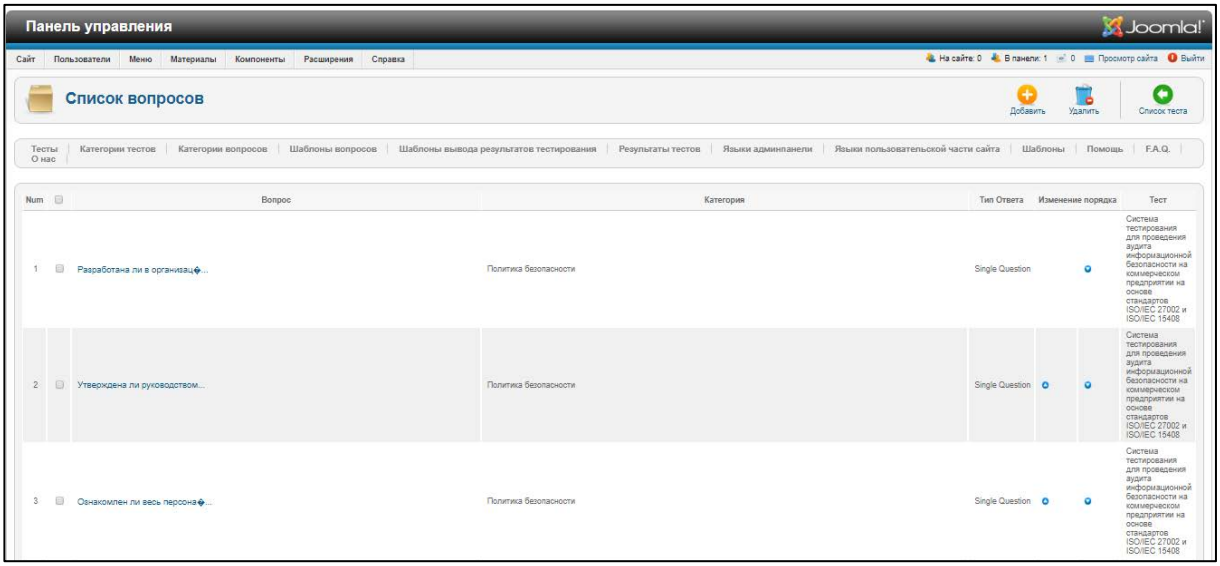


Рисунок 22 — Плагин тестирования. Разработанные варианты вопросов

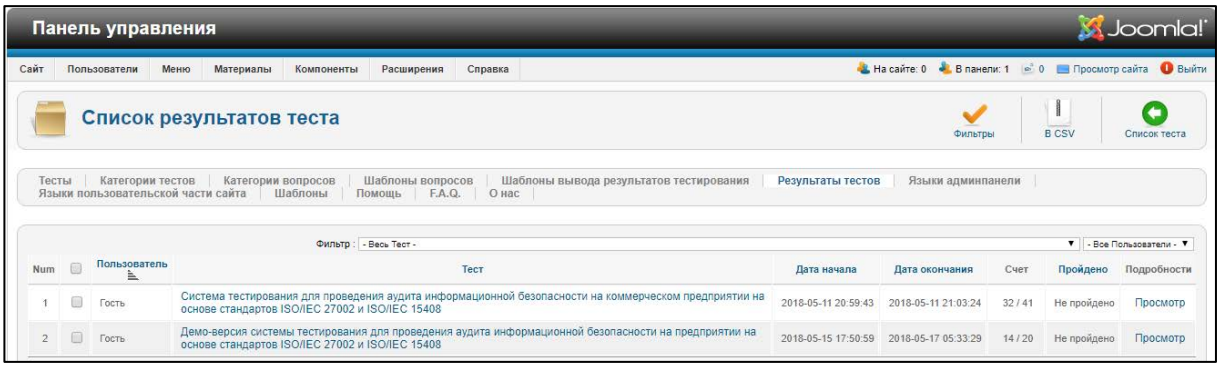


Рисунок 23 — Плагин тестирования. Список результатов пройденных ранее тестов

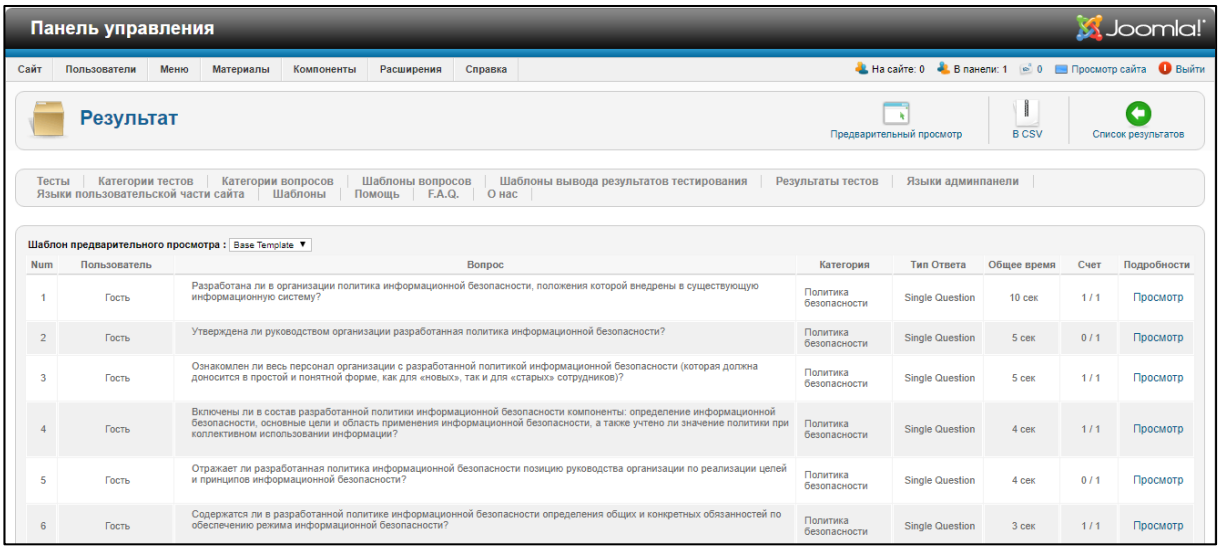


Рисунок 24 — Плагин тестирования. Результат пройденного теста с подробной формулировкой вопроса и указанием правильности выбранного варианта ответа

Банк вопросов для системы тестирования был разработан в системе управления базами данных MySQL, базы которой впоследствии были подключены к программному продукту (рисунок 25).

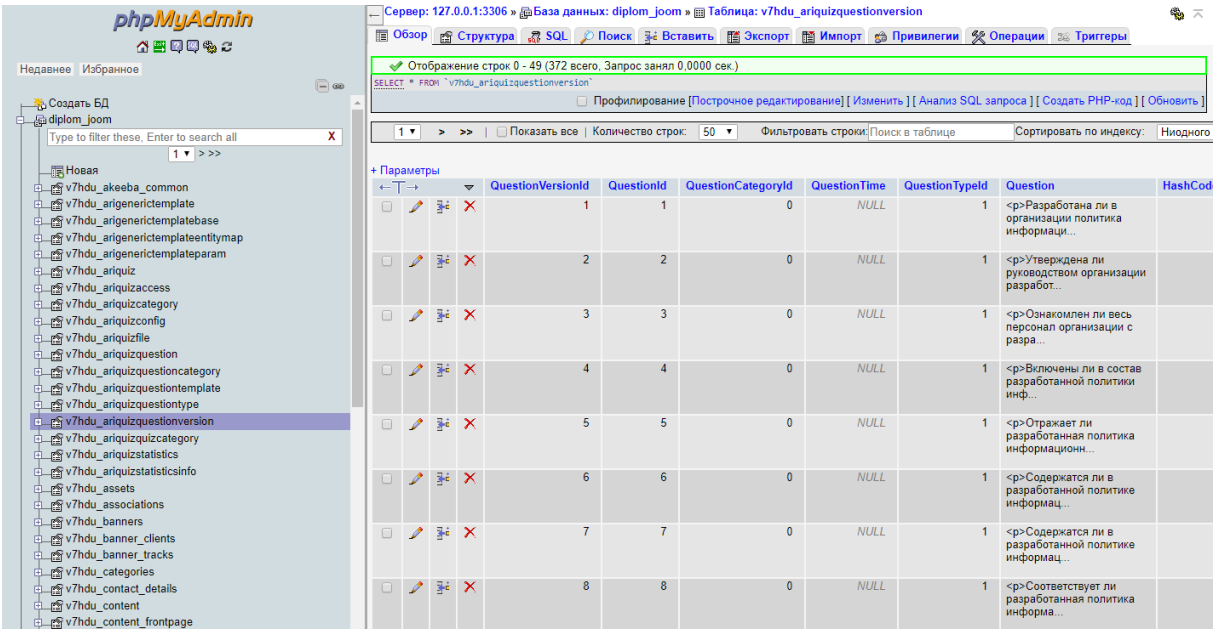


Рисунок 25 — Примеры разработанных вопросов в СУБД MySQL

2.7 Описание процедуры тестирования

В веб-приложении реализованы несколько вариантов прохождения тестирования, все зависит от статуса пользователя (гость или зарегистрированный пользователь), как говорилось ранее:

1. **Демо-версия**. Данная версия (рисунок 26, 27, 28) доступна только пользователю в статусе «Гость», поскольку предполагает ознакомление с идеей разработанного программного продукта. В состав данной версии включены 20 вопросов, которые разделены на 10 категорий (2 вопроса в каждой категории).

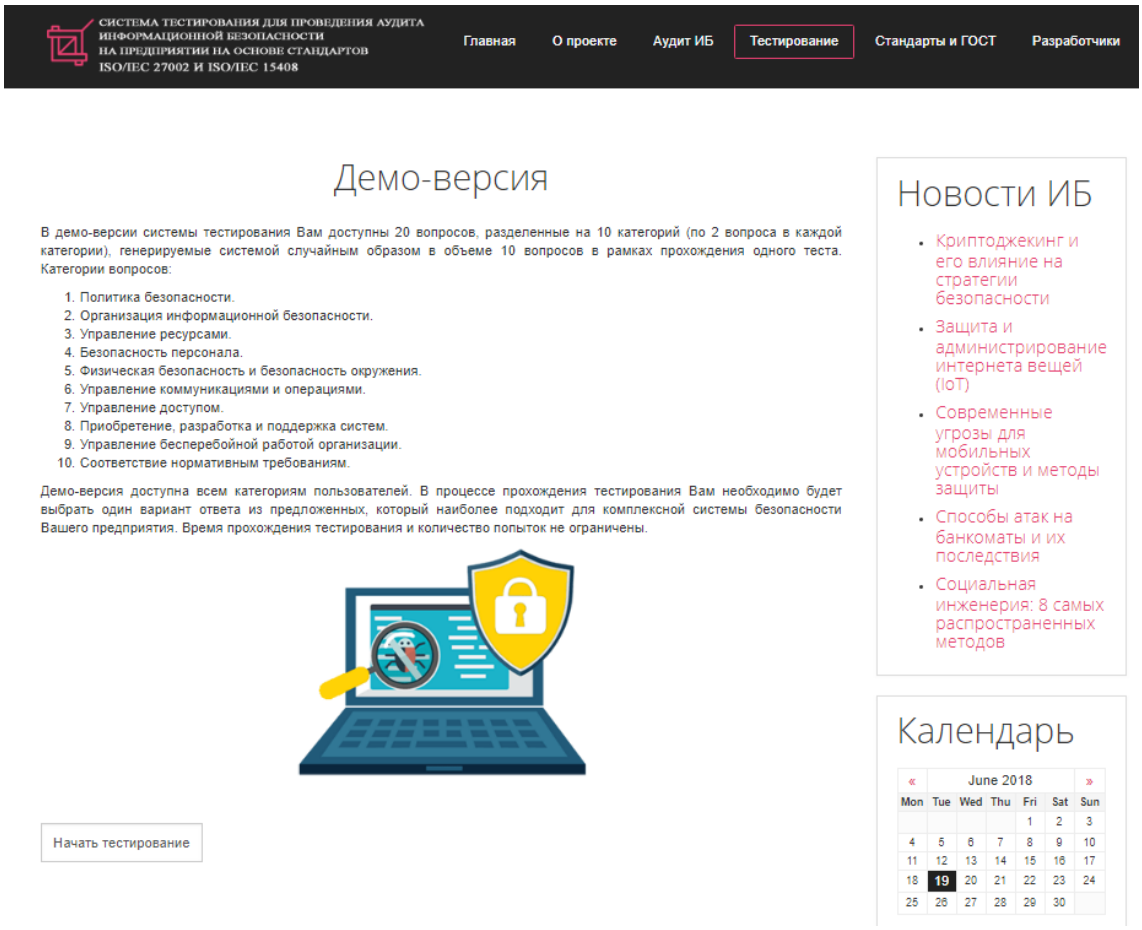


Рисунок 26 — Демо-версия системы тестирования для проведения аудита информационной безопасности на предприятии на основе стандартов ISO/IEC 27002 и ISO/IEC 15408

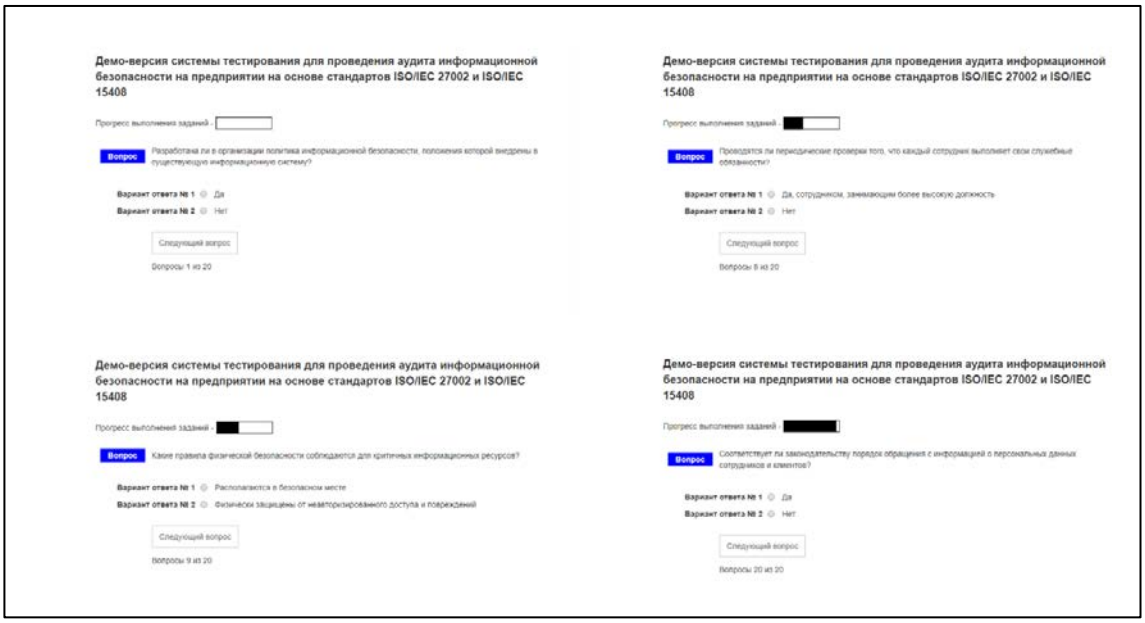
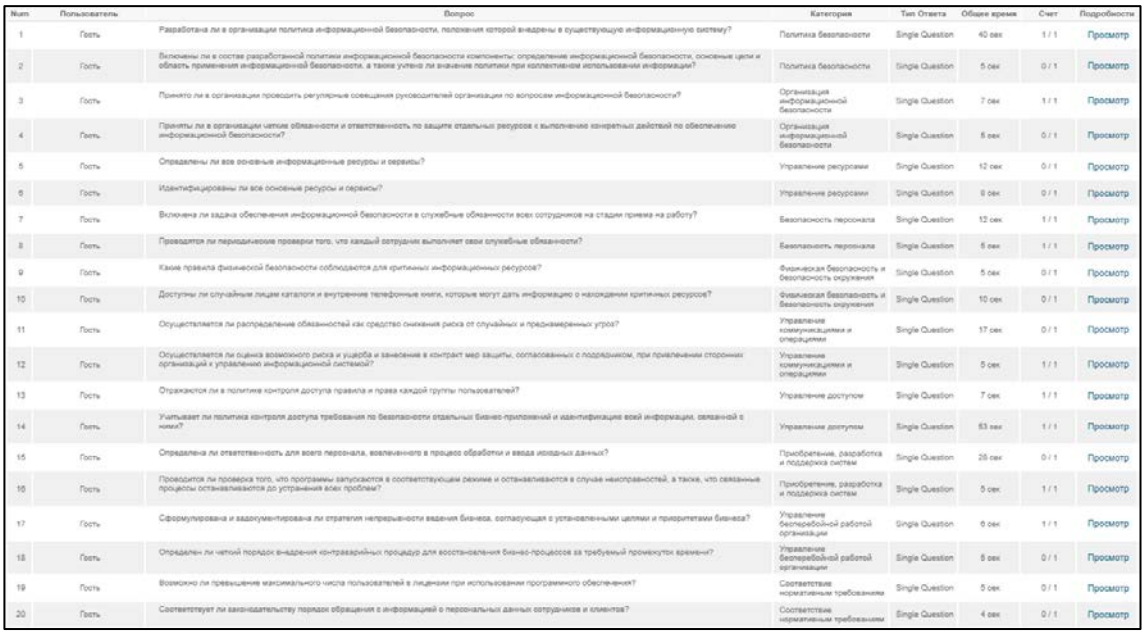


Рисунок 27 — Прохождение демо-версии системы тестирования от имени стороннего пользователя в статусе «Гость»



Num	Пользователь	Вопрос	Категория	Тип Ответа	Общее время	Счет	Подробности
1	Гость	Разработана ли в организации политика информационной безопасности, положения которой внедрены в существующую информационную систему?	Политика безопасности	Single Question	40 сек	1 / 1	Просмотр
2	Гость	Включены ли в состав разработанной политики информационной безопасности компоненты: определение информационной безопасности, основные цели и область применения информационной безопасности, а также учтено ли значение политики при коллективном использовании информации?	Политика безопасности	Single Question	5 сек	0 / 1	Просмотр
3	Гость	Принято ли в организации проводить регулярные совещания руководителей организации по вопросам информационной безопасности?	Организация информационной безопасности	Single Question	7 сек	1 / 1	Просмотр
4	Гость	Приняты ли в организации четкие обязанности и ответственность по защите отдельных ресурсов с выполнением конкретных действий по обеспечению информационной безопасности?	Организация информационной безопасности	Single Question	6 сек	0 / 1	Просмотр
5	Гость	Определены ли все основные информационные ресурсы и сервисы?	Управление ресурсами	Single Question	12 сек	0 / 1	Просмотр
6	Гость	Идентифицированы ли все основные ресурсы и сервисы?	Управление ресурсами	Single Question	8 сек	0 / 1	Просмотр
7	Гость	Включена ли задача обеспечения информационной безопасности в служебные обязанности всех сотрудников на стадии приема на работу?	Безопасность персонала	Single Question	12 сек	1 / 1	Просмотр
8	Гость	Проводятся ли периодические проверки того, что каждый сотрудник выполняет свои служебные обязанности?	Безопасность персонала	Single Question	6 сек	1 / 1	Просмотр
9	Гость	Какие правила физической безопасности соблюдаются для критичных информационных ресурсов?	Физическая безопасность и безопасность окружения	Single Question	5 сек	0 / 1	Просмотр
10	Гость	Доступны ли случайным лицам каталоги и внутренние телефонные книги, которые могут дать информацию о нахождении критичных ресурсов?	Физическая безопасность и безопасность окружения	Single Question	10 сек	0 / 1	Просмотр
11	Гость	Осуществляется ли распределение обязанностей как средство снижения риска от случайных и преднамеренных угроз?	Управление коммуникациями и операциями	Single Question	17 сек	0 / 1	Просмотр
12	Гость	Осуществляется ли оценка возможного риска и ущерба и занесение в контракт мер защиты, согласованных с подрядчиком, при привлечении сторонних организаций к управлению информационной системой?	Управление коммуникациями и операциями	Single Question	5 сек	1 / 1	Просмотр
13	Гость	Отражаются ли в политике контроля доступа правила и права каждой группы пользователей?	Управление доступом	Single Question	7 сек	1 / 1	Просмотр
14	Гость	Учитывает ли политика контроля доступа требования по безопасности отдельных бизнес-приложений и идентификация всей информации, связанной с ними?	Управление доступом	Single Question	63 сек	1 / 1	Просмотр
15	Гость	Определена ли ответственность для всего персонала, вовлеченного в процесс обработки и ввода исходных данных?	Приобретение, разработка и поддержка систем	Single Question	26 сек	0 / 1	Просмотр
16	Гость	Проводится ли проверка того, что программы запускаются в соответствующем режиме и останавливаются в случае неисправностей, а также, что связанные процессы останавливаются до устранения всех проблем?	Приобретение, разработка и поддержка систем	Single Question	5 сек	1 / 1	Просмотр
17	Гость	Сформулирована и задокументирована ли стратегия непрерывности ведения бизнеса, согласующая с установленными целями и приоритетами бизнеса?	Управление бесперебойной работой организации	Single Question	6 сек	1 / 1	Просмотр
18	Гость	Определен ли четкий порядок внедрения контраварийных процедур для восстановления бизнес-процессов за требуемый промежуток времени?	Управление бесперебойной работой организации	Single Question	5 сек	0 / 1	Просмотр
19	Гость	Возможно ли превышение максимального числа пользователей в лицензии при использовании программного обеспечения?	Соответствие нормативным требованиям	Single Question	5 сек	0 / 1	Просмотр
20	Гость	Соответствует ли законодательству порядок обращения с информацией о персональных данных сотрудников и клиентов?	Соответствие нормативным требованиям	Single Question	4 сек	0 / 1	Просмотр

Рисунок 28 — Пример отображения отчета о пройденном тестировании с отображением результатов пройденного демо-теста от имени стороннего пользователя в статусе «Гость»

2. **Тестирование по полному сценарию** (рисунок 29) коммерческих предприятий и образовательных организаций. Данная процедура предполагает прохождение 325 вопросов, разделенные на 10 разделов, доступ к которой возможен после прохождения регистрации и авторизации на сайте (рисунок 8, 9).

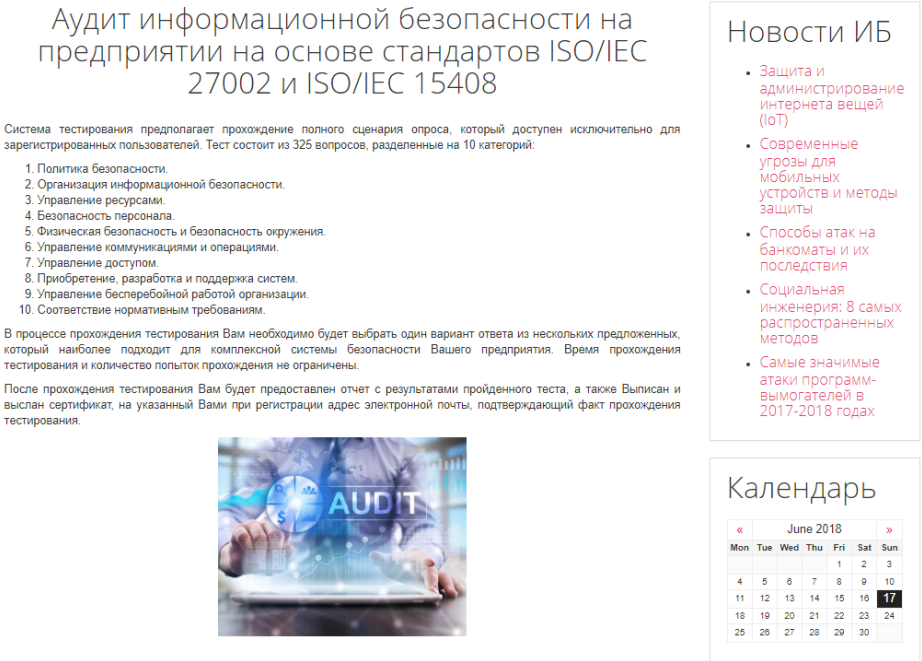


Рисунок 29 — Панель системы тестирования для проведения аудита информационной безопасности на основе стандартов ISO/IEC 27002 и ISO/IEC 15408

3. **Тестирование по отдельным категориям**. При выборе данного варианта прохождения тестирования через веб-приложение (рисунок 30), зарегистрированному пользователю будут доступны все категории тестов (таблица 1), с включенными в них вопросами, которые задействованы при прохождении тестирования по полному сценарию. Отличие состоит лишь в том, что пользователь самостоятельно сможет выбрать ту категорию, которая будет ему наиболее интересна, и самостоятельно сможет оценить существующие на его предприятии риски по выбранной категории.

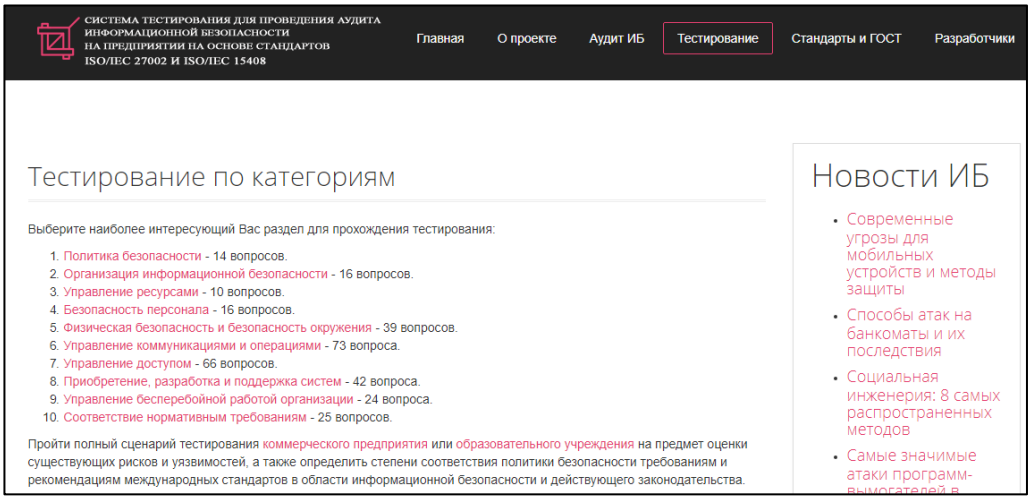


Рисунок 30 — Страница выбора категории для прохождения тестирования

И в том, и другом случае плагин выдает пользователю определенный вид теста, который необходимо пройти. В процессе прохождения тестирования плагин анализирует полученные ответы и сравнивает их с эталоном (определяется соответствие того или иного параметра описанным в стандартах требованиях).

После прохождения теста, на указанный электронный адрес при регистрации предприятия на сайте высылается полный отчет по пройденной процедуре тестирования, в котором содержится следующая информация:

- общее количество набранных баллов (максимально возможное количество баллов — 325, по 1 баллу за эталонное значение (на основании данных международных стандартов);

- количество набранных баллов по разделу (максимально возможное количество баллов зависит от количества вопросов по определенной категории);
- подробная формулировка вопроса и выбранный уполномоченным лицом от предприятия вариант ответа (неверно выбранный вариант ответа, определяет нарушение требованиях стандарта по информационной безопасности и указывает на наличие определенного риска или угрозы для системы безопасности предприятия, как отдельным ее частям, так и для комплексной системы защиты).

На основании полученных данных система тестирования формирует отчет, в котором прописывается общее количество набранных баллов исходя из логики: соответствует ли полученный ответ требованиям или рекомендациям международных стандартов в области информационной безопасности. В отчете прописывается формулировка вопроса, и ответ пользователя к нему. Не трудно догадаться, что если ответ пользователя был отмечен как «неверный», то именно эта позиция в системе комплексной системы безопасности предприятия требует пересмотра или доработки. Результат прохождения тестирования хранится в базе данных программного продукта. Результат пройденного теста, наглядно отражает возможные риски и угрозы для предприятия, по которому в дальнейшем строятся рекомендации по их предотвращению и дальнейшему предупреждению.

На основании полученной информации, которая выдается по результатам пройденного тестирования (рисунок 28), руководством компании могут быть приняты дополнительные меры по совершенствованию существующей системы информационной безопасности.

На примере пройденного демо-теста (рисунок 27) и полученного результата прохождения к нему (рисунок 28) опишем процедуру анализа полученных данных (таблица 2) на предмет выявления существующих уязвимостей на условном предприятии с условно определенной его системой безопасности.

Составленные рекомендации, соответствуют международному стандарту ISO/IEC 27002, поэтому могут использоваться руководством предприятия для совершенствования политики безопасности и формирования определенных инструкций и правил для персонала внутри организации.

Таблица 2 — Пример рекомендаций условному предприятию

№	Вопрос	Счет	Рекомендация
1	Разработана ли в организации политика информационной безопасности, положения которой внедрены в существующую информационную систему?	1	Полученный ответ, соответствует рекомендациям международных стандартов в области информационной безопасности.
2	Включены ли в состав разработанной политики информационной безопасности компоненты: определение информационной безопасности, основные цели и область применения информационной безопасности, а также учтено ли значение политики при коллективном использовании информации?	0	Компании рекомендуется: 1. Проработать и утвердить формулировку термину ИБ. 2. Определить основные цели, задачи, перспективные направления и область применения политики ИБ. 3. Определить порядок и уровни доступа использования ресурсов и информации в компании.
3	Принято ли в организации проводить регулярные совещания руководителей организации по вопросам информационной безопасности?	1	Полученный ответ, соответствует рекомендациям международных стандартов в области информационной безопасности.
4	Приняты ли в организации четкие обязанности и ответственность по защите отдельных ресурсов к выполнению конкретных действий по обеспечению информационной безопасности?	0	Компании рекомендуется: 1. Принять четкие обязанности и четко определить степень ответственности персонала по защите отдельных ресурсов к выполнению конкретных действий по обеспечению информационной безопасности.
5	Определены ли все основные информационные ресурсы и сервисы?	0	Компании рекомендуется: 1. Определить все основные используемые и затрагиваемые при работе информационные ресурсы и сервисы.
6	Идентифицированы ли все основные ресурсы и сервисы?	0	Компании рекомендуется: 1. Идентифицировать все основные используемые и затрагиваемые при работе информационные ресурсы и сервисы.
7	Включена ли задача обеспечения информационной безопасности в	1	Полученный ответ, соответствует рекомендациям международных

	служебные обязанности всех сотрудников на стадии приема на работу?		стандартов в области информационной безопасности.

Продолжение таблицы 2

8	Проводятся ли периодические проверки того, что каждый сотрудник выполняет свои служебные обязанности?	1	Полученный ответ, соответствует рекомендациям международных стандартов в области информационной безопасности.
9	Какие правила физической безопасности соблюдаются для критичных информационных ресурсов?	0	Компании рекомендуется: 1. Обеспечить должный уровень безопасности для критичных информационных ресурсов компании, путем обеспечения их физической защиты от неавторизированного доступа и повреждений и хранением в безопасном месте.
10	Доступны ли случайным лицам каталоги и внутренние телефонные книги, которые могут дать информацию о нахождении критичных ресурсов?	0	Компании рекомендуется: 1. Обеспечить должный уровень защиты каталогов, внутренних телефонных книг, журналов, а также другой внутренней документации о нахождении критичных ресурсов от доступа к ним третьих лиц.
11	Осуществляется ли распределение обязанностей как средство снижения риска от случайных и преднамеренных угроз?	0	Компании рекомендуется: 1. Распределить обязанности среди сотрудников компании по обеспечению должного уровня информационной безопасности с целью снижения риска от случайных или преднамеренных угроз.
12	Осуществляется ли оценка возможного риска и ущерба и занесение в контракт мер защиты, согласованных с подрядчиком, при привлечении сторонних организаций к управлению информационной системой?	1	Полученный ответ, соответствует рекомендациям международных стандартов в области информационной безопасности.
13	Отражаются ли в политике контроля доступа правила и права каждой группы пользователей?	1	Полученный ответ, соответствует рекомендациям международных стандартов в области информационной безопасности.
14	Учитывает ли политика контроля доступа требования по безопасности отдельных бизнес-приложений и идентификацию всей информации, связанной с ними?	1	Полученный ответ, соответствует рекомендациям международных стандартов в области информационной безопасности.
15	Определена ли ответственность для всего персонала, вовлеченного в процесс обработки и ввода исходных данных?	0	Компании рекомендуется: 1. Определить ответственность для всего персонала компании, вовлеченного в процесс обработки и ввода исходных данных.
16	Проводится ли проверка того, что программы запускаются в соответствующем режиме и останавливаются в случае неисправностей, а также, что	1	Полученный ответ, соответствует рекомендациям международных стандартов в области информационной безопасности.

	связанные процессы останавливаются до устранения всех проблем?		

Окончание таблицы 2

17	Сформулирована и задокументирована ли стратегия непрерывности ведения бизнеса, согласующая с установленными целями и приоритетами бизнеса?	1	Полученный ответ, соответствует рекомендациям международных стандартов в области информационной безопасности
18	Определен ли четкий порядок внедрения контраварийных процедур для восстановления бизнес-процессов за требуемый промежуток времени?	0	Компании рекомендуется: 1. Определить и утвердить четкий порядок внедрения контраварийных процедур для восстановления бизнес-процессов компании за требуемый промежуток времени.
19	Возможно ли превышение максимального числа пользователей в лицензии при использовании программного обеспечения?	0	Компании рекомендуется: 1. Использовать внутри организации лицензионное программное обеспечение, с его установкой и эксплуатацией без превышения максимального числа пользователей.
20	Соответствует ли законодательству порядок обращения с информацией о персональных данных сотрудников и клиентов?	0	Компании рекомендуется: 1. Привести в норму порядок обращения с информацией о персональных данных сотрудников и клиентов в соответствии с действующим законодательством.

2.8 Использование системы тестирования в образовательном процессе

Использовать разработанный программный продукт можно в образовательном процессе при обучении студентов по следующим направлениям подготовки: 44.03.04 Профессиональное обучение (по отраслям), профиль подготовки «Информатика и вычислительная техника», профилизация «Информационная безопасность»; 10.03.01 Информационная безопасность; 38.04.09 Государственный аудит и т. п., задействовав его практическую направленность при изучении тем, связанных с аудитом информационной безопасности на предприятиях, международными и национальными стандартами РФ в области информационной безопасности (например: ISO/IEC 27002,

ГОСТ Р ИСО/МЭК 27002 и др.), при наработке практических навыков по методике поиска, анализа рисков и управления ими.

Для использования продукта в процессе обучения дисциплины «Политика безопасности предприятия» необходимо развернуть локальную версию программного продукта на персональном компьютере и использовать его как обзорный и интуитивно понятный инструмент по поиску и анализу рисков в системе безопасности предприятия: как конкретных, так и условно заданных преподавателями в рамках прохождения контрольных и самостоятельных работ после изучения теоретического материала по темам, связанным с аудитом информационной безопасности; планированием, разработкой и проведением мероприятий по защите информации в организациях и т. д.

Для возможности использования программного продукта в образовательном процессе, был отдельно сформирован архив, в который была упакована его локальная версия. Для установки локальной версии потребуется предварительно установить на персональный компьютер OpenServer, с целью дальнейшего развертывания архива, установки баз и управления программным продуктом.

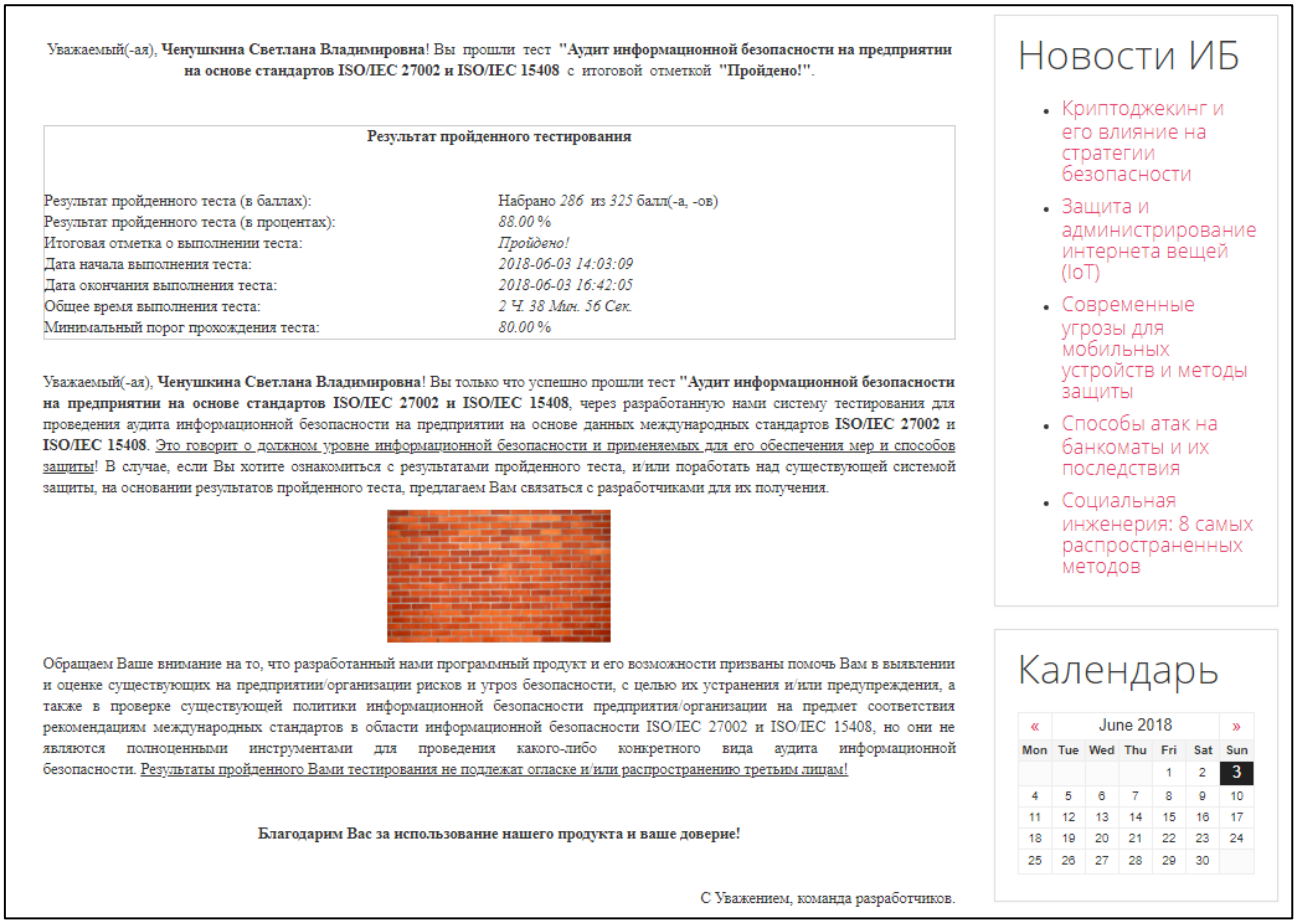
2.9 Апробация продукта

2.9.1 Апробация продукта в образовательном учреждении

Разработанный программный продукт прошел апробацию в Федеральном государственном автономном образовательном учреждении (ФГАОУ) высшего образования (ВО) «Российский государственный профессионально-педагогический университет» (РГППУ) в центре Веб-технологий и программирования. Руководитель центра — Ченушкина Светлана Владимировна, прошла предлагаемый веб-приложением тест для образовательных учреждений. Полученный результат не подлежит огласке, но в рамках его вынесения в итоги выпускной квалификационной работы, стоит отметить, что уровень состояние ин-

формационной безопасности и степени соответствия используемых в нем систем защиты — высокий. Результат оценивается в 88% от 100%, при необходимом минимальном пороге прохождения 80% (рисунок 31).

Подробный результат о пройденном тестировании в отделе веб-технологий и программирования в ФГАОУ ВО РГППУ:



Уважаемый(-ая), **Ченушкина Светлана Владимировна**! Вы прошли тест **"Аудит информационной безопасности на предприятии на основе стандартов ISO/IEC 27002 и ISO/IEC 15408** с итоговой отметкой **"Пройдено!"**.

Результат пройденного тестирования

Результат пройденного теста (в баллах):	Набрано *286* из *325* балл(-а, -ов)
Результат пройденного теста (в процентах):	*88.00* %
Итоговая отметка о выполнении теста:	*Пройдено!*
Дата начала выполнения теста:	*2018-06-03 14:03:09*
Дата окончания выполнения теста:	*2018-06-03 16:42:05*
Общее время выполнения теста:	*2 Ч. 38 Мин. 56 Сек.*
Минимальный порог прохождения теста:	*80.00* %

Уважаемый(-ая), **Ченушкина Светлана Владимировна**! Вы только что успешно прошли тест **"Аудит информационной безопасности на предприятии на основе стандартов ISO/IEC 27002 и ISO/IEC 15408**, через разработанную нами систему тестирования для проведения аудита информационной безопасности на предприятии на основе данных международных стандартов **ISO/IEC 27002** и **ISO/IEC 15408**. Это говорит о должном уровне информационной безопасности и применяемых для его обеспечения мер и способов защиты! В случае, если Вы хотите ознакомиться с результатами пройденного теста, и/или поработать над существующей системой защиты, на основании результатов пройденного теста, предлагаем Вам связаться с разработчиками для их получения.

Обращаем Ваше внимание на то, что разработанный нами программный продукт и его возможности призваны помочь Вам в выявлении и оценке существующих на предприятии/организации рисков и угроз безопасности, с целью их устранения и/или предупреждения, а также в проверке существующей политики информационной безопасности предприятия/организации на предмет соответствия рекомендациям международных стандартов в области информационной безопасности ISO/IEC 27002 и ISO/IEC 15408, но они не являются полноценными инструментами для проведения какого-либо конкретного вида аудита информационной безопасности. Результаты пройденного Вами тестирования не подлежат огласке и/или распространению третьим лицам!

Благодарим Вас за использование нашего продукта и ваше доверие!

С Уважением, команда разработчиков.

Новости ИБ

- Криптоджекинг и его влияние на стратегии безопасности
- Защита и администрирование интернета вещей (IoT)
- Современные угрозы для мобильных устройств и методы защиты
- Способы атак на банкоматы и их последствия
- Социальная инженерия: 8 самых распространенных методов

Календарь

« June 2018 »

Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Рисунок 31 — Результат пройденного тестирования в отделе веб-технологий и программирования ФГАОУ ВО РГППУ

На основе анализа полученных результатов были определены следующие риски в образовательной организации:

1. **Защита данных пользователей**. Обусловлено большим количеством сотрудников, с характерным для них постоянным перемещением (переселением по кабинетам). Большим количеством студентов, пользующихся сетью и ресурсами образовательной организации.

2. **Управление информационной безопасностью**. Обусловлено отсутствием единого отдела, который был бы уполномочен заниматься информационной безопасностью и управлять правами доступа сотрудников, отделов к ресурсам в образовательной организации, а также наличием разрозненности структурных подразделений образовательной организации, отвечающих за безопасность.

3. **Каналы передачи информации**. Использование безопасных протоколов отправки министерской отчетности, основанных на применении шифрования, в противовес недостаточно надежных и уязвимых протоколов обмена внутренне-организационной информацией между структурными и территориальными подразделениями образовательной организации (например, **RDP** (Remote Desktop Protocol — протокол удалённого рабочего стола)).

После прохождения тестирования по полному сценарию, через веб-приложение, выдается подтверждающий сертификат (рисунок 32).

Рисунок 32 — Сертификат за прохождение тестирования

2.9.2 Апробация в учебном процессе

Разработанный программный продукт был апробирован в образовательном процессе группы ЗИБ-401. Данной учебной группой была изучена дисциплина «Защита сетевых информационных систем» в рамках программы подго-

товки академического бакалавриата, по направлению подготовки 44.03.04 Профессиональное обучение (по отраслям), профиль подготовки «Информатика и вычислительная техника», профилизация «Информационная безопасность», в программе которой содержалась глава, посвященная аудиту информационной безопасности на предприятии. Поскольку большинство студентов-заочников являются сотрудниками организаций и предприятий различного уровня, им было предложено выполнить курсовую работу по дисциплине «Защита сетевых информационных систем», используя возможности программного продукта. В рамках выполнения курсовой работы студентам было предложено выступить в роли условных аудиторов своего предприятия, с целью закрепления изученного теоретического материала, применения его на практике, получения навыков по методике поиска и анализа рисков, без разглашения результатов и какой-либо сторонней информации, содержащей коммерческую тайну и способной нанести ущерб предприятию. Согласно условиям выполнения, студенты получили на руки методические указания к выполнению курсовой работы, содержащие в плане анализа деятельности предприятия пункт «Аудит информационной безопасности предприятия».

Для студентов выделяются два академических часа аудиторной работы из программы прохождения дисциплины. Предварительно, на каждый персональный компьютер в учебном классе, согласно количеству человек в группе, разворачивается локальная версия программного продукта «Система тестирования для проведения аудита информационной безопасности на предприятии на основе стандартов ISO/IEC 27002 и ISO/IEC 15408», в котором студентам предстоит индивидуально выполнить работу по оценке и анализу деятельности предприятия, зарегистрировавшись и пройдя тестирование в веб-приложении, как работник предприятия. Основанием, подтверждающим факт прохождения тестирования, является занесение студентами в отчет по выполненной работе процентного соотношения надежности систем информационной безопасности предприятия и степени их соответствия рекомендациям международных стандартов в

области информационной безопасности без указания какой-либо уточняющей информации. Так, студент группы ЗИБ-401 Максим Ефремов, использовал возможности программного продукта при выполнении курсовой работы по дисциплине «Защита сетевых информационных систем» на тему «Анализ безопасности предприятия ООО ИНСИС», будучи его сотрудником.

Хочется отметить, что работа проводилась студентами в локальной версии программного продукта на персональных компьютерах, не через онлайн версию веб-приложения, с целью предупреждения фактов нарушения требований действующего законодательства о защите и охране персональных данных, в том числе данных, содержащих коммерческую тайну.

ЗАКЛЮЧЕНИЕ

В заключение хотелось бы сказать о том, что все поставленные в выпускной квалификационной работе задачи были решены в полном объеме. Цель достигнута. В результате выполнения выпускной квалификационной работы были разработаны:

1. **Веб-приложение** (сверстанный шаблон для системы управления содержимым с открытым исходным кодом — Joomla (версия 2.5.17)).
2. **Плагин тестирования** (исправленный и доработанный функционал плагина тестирования — ARI Quiz).
3. **Банк вопросов**, состоящий из 325 вопросов (закрытой формы с выбором одного варианта ответа по принципу классификации), распределенными на 10 категорий, на основе данных международных стандартов ISO/IEC 27002 и ISO/IEC 15408, нацеленные на выявление и оценку рисков информационной безопасности в компаниях. Возможности программного продукта предполагают прохождение тестирования как коммерческими предприятиями, так и образовательными организациями, с учетом характерной для них специфики.

Хочется отметить, что прохождение тестирования на основе использования данного программного продукта не является «внутренним» аудитом информационной безопасности. Его возможности прежде всего нацелены на выявление «слабых» мест в системе безопасности организации, с целью проверки качества информационной безопасности в организации. Полученная информация впоследствии может быть использована для проведения каких-либо дополнительных мер по улучшению как комплексной, так и отдельных систем защиты, политики информационной безопасности в организации или самостоятельной подготовки к аудиту, поскольку продукт основан на используемых аудиторами международных стандартах в области информационной безопасности

ISO/IEC 27002 и ISO/IEC 15408 и проверяет часть предъявляемых стандартами и проверяемых аудиторами требований, и критериев в организации.

В процессе работы над выпускной квалификационной работой были решены следующие задачи:

- была проанализирована литература и интернет-источники по аудиту и менеджменту информационной безопасности, анализу и управлению рисками на предприятиях;
- были изучены международные стандарты в области информационной безопасности;
- был разработан банк тестовых вопросов по международным стандартам информационной безопасности ISO/IEC 27002 и ISO/IEC 15408;
- было разработано веб-приложение и доработан функционал существующего плагина тестирования для проведения интернет-тестирования с возможностью авторизированного доступа, вывода результатов тестирования и круглосуточного доступа к нему.

Проведение оценки рисков информационной безопасности в организации является одним из наиболее эффективных инструментов по получению объективной информации о текущем уровне защищенности от всевозможных угроз, с целью их предупреждения и избежание ущерба. Именно поэтому оценка рисков на предприятиях различного уровня должна проводится на регулярной основе специалистами или руководством организации для достижения максимальной отдачи и повышения уровня информационной безопасности организации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Anti-Malware — информационная безопасность для профессионалов // Anti-Malware [Электронный ресурс] — Режим доступа — http://www.anti-malware.ru (дата обращения: 26.05.2018).
2. ARI Quiz Lite — Мощный компонент для организации тестов на сайте // Alekseygen [Электронный ресурс] — Режим доступа — http://alekseygen.ru/joomla-2-5/komponenty/15-ari-quiz-lite-moshchnyj-komponent-dlya-organizatsii-testov-na-sajte-rusifikatsiya.html (дата обращения: 03.06.2018).
3. Drupal // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/Drupal (дата обращения: 27.05.2018).
4. Joomla // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/Joomla! (дата обращения: 27.05.2018).
5. Joomla! Quiz Deluxe компонент для создания тестов, онлайн-опросников и викторин // Центр обучения Joomla [Электронный ресурс] — Режим доступа — https://alex-kurteev.ru/extensions/full/26-oprosy/1201-joomla-quiz-deluxe-joomla-komponent-dlya-sozdaniya-testov.html (дата обращения: 03.06.2018).
6. WordPress // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/WordPress (дата обращения: 27.05.2018).
7. Аверченков В.И. Аудит информационной безопасности [Текст]: учебное пособие для вузов / В.И. Аверченков. — 3-е изд., стереотип. — Москва: ФЛИНТА, 2016. — 269 с.
8. Анализ рисков в управлении информационной безопасностью // Искусство управления информационной безопасностью ISO27000 [Электронный ресурс] — Режим доступа — http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/analiz-riskov-v-upravlenii-informacionnoi-bezopasnostyu (дата обращения: 22.05.2018).

9. Аудит безопасности информационных систем // Искусство управления информационной безопасностью ISO27000 [Электронный ресурс] — Режим доступа — http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti (дата обращения: 22.05.2018).

10. Аудит информационной безопасности — основа эффективной защиты предприятия // ДиалогНаука [Электронный ресурс] — Режим доступа — https://dialognauka.ru/press-center/article/4753/ (дата обращения: 01.04.2018).

11. Аудит информационной безопасности // IBS [электронный ресурс] — Режим доступа — https://www.ibs.ru/it-infrastructure/information-security/audit-informatsionnoy-bezopasnosti/ (дата обращения: 23.05.2018).

12. Аудит информационной безопасности // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/Аудит_информационной_безопасности (дата обращения: 22.05.2018).

13. Аудит информационной безопасности // Контур [Электронный ресурс] — Режим доступа — https://kontur.ru/security/features/audit-ib/ (дата обращения: 23.05.2018).

14. Аудит информационной безопасности. Анализ защищенности систем и приложений // Pentestit [Электронный ресурс] — Режим доступа — https://www.pentestit.ru/audit/ (дата обращения: 23.05.2018).

15. Аудит корпоративной безопасности // Group-IB [Электронный ресурс] — Режим доступа — https://www.group-ib.ru/audit.html (дата обращения: 23.05.2018).

16. Виды аудита информационной безопасности // Искусство управления информационной безопасностью ISO27000 [Электронный ресурс] — Режим доступа — http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/vidy-audita-informacionnoi-bezopasnosti (дата обращения: 22.05.2018).

17. ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] — Режим доступа — http://docs.cntd.ru/document/1200071694 (дата обращения 25.05.2018).

18. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] — Режим доступа — http://docs.cntd.ru/document/1200105710 (дата обращения 25.05.2018).

19. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] — Режим доступа — http://docs.cntd.ru/document/1200105711 (дата обращения 25.05.2018).

20. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] — Режим доступа — http://docs.cntd.ru/document/1200058325 (дата обращения 25.05.2018).

21. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] — Режим доступа — http://docs.cntd.ru/document/1200103619 (дата обращения 26.05.2018).

22. Обследование (аудит) ИСПДн // Контур [Электронный ресурс] — Режим доступа — https://kontur.ru/security/features/ispdn/ (дата обращения: 23.05.2018).

23. Общие критерии оценки защищенности информационных технологий, Общие критерии // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/Общие_критерии#Общие_критерии_в_России/ (дата обращения: 24.05.2018).

24. Практическое применение международного стандарта информационной безопасности ISO 17799 // CitForum [Электронный ресурс] — Режим доступа — http://citforum.ru/security/articles/aboutisonew.shtml (дата обращения: 25.05.2018).

25. Программные средства аудита безопасности // StudFiles [Электронный ресурс] — Режим доступа — https://studfiles.net/preview/3508678/page:2/ (дата обращения: 24.05.2018).

26. Программные средства проверки политики безопасности на соответствие ISO 17799 // IXBT [Электронный ресурс] — Режим доступа — https://www.ixbt.com/cm/iso17799-cobra-kondor012004.shtml (дата обращения: 24.05.2018).

27. Риски информационной безопасности // ARinteg [Электронный ресурс] — Режим доступа — https://arinteg.ru/articles/riski-informatsionnoy-bezopasnosti-26222.html (Дата обращения: 23.05.2018).

28. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности [Текст]: учебное пособие / Ю.А. Родичев. — Санкт-Петербург: Питер, 2017 — 256 с.

29. Сердюк В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Текст]: учебное пособие для вузов / В.А. Сердюк. — Москва: ГУ-ВШЭ, 2011 — 576 с.

30. Сертификация по ISO 27001 // Digital Security [Электронный ресурс] — Режим доступа — https://dsec.ru/certification/iso-27001/ (дата обращения: 24.05.2018).

31. Стандарт BS 7799-1 // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/BS_7799-1/ (дата обращения: 26.05.2018).

32. Стандарт ISO/IEC 15408 // Википедия [Электронный ресурс] — Режим доступа — http://www.lghost.ru/lib/security/kurs2/theme02_chapter04.htm/ (дата обращения: 26.05.2018).

33. Стандарт ISO/IEC 17799 // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/ISO/IEC_17799/ (дата обращения: 26.05.2018).

34. Стандарт ISO/IEC 27001 // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/ISO/IEC_27001/ (дата обращения: 26.05.2018).

35. Стандарт на страже информационной безопасности // InformationSecurity [Электронный ресурс] — Режим доступа — http://www.itsec.ru/articles2/pravo/standart_na_strazhe (дата обращения: 25.05.2018).

36. Тестирование, как метод контроля качества усвоения учебного материала учащимися // Педагогическая мастерская [Электронный ресурс] — Режим доступа — http://открытыйурок.рф/статьи/500954/ (дата обращения: 23.05.2018)

37. Уязвимости: рекомендации по выработке и проведению мер по исправлению ситуации // ДиалогНаука [Электронный ресурс] — Режим доступа — https://www.dialognauka.ru/press-center/article/16761/ (дата обращения: 24.05.2018).

38. Ярочкин В.И. Аудит безопасности фирмы: теория и практика [Текст]: учебное пособие для вузов / В.И. Ярочкин, Я.В. Бузанова. — Москва: Академический проект, 2005. — 352 с.

ПРИЛОЖЕНИЕ А

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

«_____»_____20 ___ г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студента 4 курса, группы ИБ-401 **Филиппова Ивана Евгеньевича**

1. Тема «Система тестирования для проведения аудита информационной безопасности на предприятии на основе международных стандартов» утверждена распоряжением по институту от ___.___.2018 г. г. № ___.

2. Руководитель **Ченушкина Светлана Владимировна**, старший преподаватель кафедры ИС.

3. Место преддипломной практики **ФГАОУ ВО «Российский государственный профессионально-педагогический университет».**

4. Исходные данные к ВКР:

- Аверченков В.И. Аудит информационной безопасности [Текст]: учебное пособие для вузов;
- Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности [Текст]: учебное пособие;
- Анализ рисков в управлении информационной безопасностью // Искусство управления информационной безопасностью ISO27000 [Электронный ресурс] — Режим доступа — http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/analiz-riskov-v-upravlenii-informacionnoi-bezopasnostyu;
- ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] — Режим доступа — http://docs.cntd.ru/document/1200103619.

5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов):

- анализ литературы и интернет-источников;
- изучение международных стандартов информационной безопасности;
- разработка банка тестовых вопросов по стандарту ISO/IEC 27002;
- разработка интернет-сайта;
- разработка интерфейса для проведения интернет-тестирования.

6. Перечень демонстрационных материалов:

- интернет-сайт «Система тестирования для проведения аудита информационной безопасности на предприятии на основе стандартов ISO/IEC 27002 и ISO/IEC 15408»;
- презентация, выполненная в Microsoft PowerPoint.

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа ВКР	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной работе и сдача зачета по преддипломной практике	21.05.2018	15%	
2	Выполнение работ по разрабатываемым вопросам их изложение в выпускной работе		65%	
2.1	Анализ литературы и интернет-источников	22.05.2018	10%	
2.2	Изучение международных стандартов информационной безопасности	25.05.2018	10%	
2.3	Разработка банка тестовых вопросов по стандарту ISO/IEC 27002	28.05.2018	30%	
2.4	Разработка интернет-сайта	01.05.2018	10%	
2.5	Доработка и функционала плагина тестирования	05.06.2018	5%	
3	Оформление текстовой части ВКР	10.06.2018	5%	
4	Выполнение демонстрационного материала к ВКР	11.06.2018	5%	
5	Нормоконтроль	12.06.2018	5%	
6	Подготовка доклада к защите в ГЭК	13.06.2018	5%	

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 **Филиппова И. Е.** к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

Руководитель _____ _____
подпись дата

10. Допустить **Филиппова И. Е.** к защите выпускной квалификационной работы в государственной экзаменационной комиссии (протокол заседания кафедры от ___.___.2018 г. №___)

Заведующий кафедрой _____ _____
подпись дата

ПРИЛОЖЕНИЕ Б

Примеры разработанных вопросов по разделам банка вопросов

Таблица Б.1 — Примеры разработанных вопросов по разделам банка вопросов

Название раздела	Формулировка вопроса	Варианты ответа
Политика безопасности	1. Разработана ли в организации политика информационной безопасности, положения которой внедрены в существующую информационную систему?	• **Да (верно)** • Нет
	2. Включены ли в состав разработанной политики информационной безопасности компоненты: определение информационной безопасности, основные цели и область применения информационной безопасности, а также учтено ли значение политики при коллективном использовании информации?	• **Да (верно)** • Нет
	3. Отражает ли разработанная политика информационной безопасности позицию руководства организации по реализации целей и принципов информационной безопасности?	• **Да (верно)** • Нет
Организация информационной безопасности	1. Принято ли в организации проводить регулярные совещания руководителей организации по вопросам информационной безопасности?	• **Да (верно)** • Нет
	2. Приняты ли в организации четкие обязанности и ответственность по защите отдельных ресурсов к выполнению конкретных действий по обеспечению информационной безопасности?	• **Да (верно)** • Нет
	3. Заключается ли договор со сторонними компаниями при их доступе к ресурсам организации, в котором согласованы и зафиксированы процедуры проверки?	• **Да (верно)** • Нет
Управление ресурсами	1. Определены ли все основные информационные ресурсы и сервисы?	• **Да (верно)** • Нет
	2. Идентифицированы ли все основные ресурсы и сервисы?	• **Да (верно)** • Нет
	3. Есть ли определенные обязанности между владельцами информационных ресурсов, направленные на поддержание соответствующего уровня информационной безопасности организации?	• **Да (верно)** • Нет

Продолжение таблицы Б.1

Безопасность персонала	1. Включена ли задача обеспечения информационной безопасности в служебные обязанности всех сотрудников на стадии приема на работу?	• **Да (верно)** • Нет
	2. Проводятся ли периодические проверки того, что каждый сотрудник выполняет свои служебные обязанности?	• **Да, сотрудником, занимающим более высокую должность (верно)** • Нет
	3. Проводится ли проверка репутации сотрудников, работающих по контракту, и временных служащих?	• **Да (верно)** • Нет
Физическая безопасность и безопасность окружения	1. Какие правила физической безопасности соблюдаются для критичных информационных ресурсов?	• Располагаются в безопасном месте • **Физически защищены от неавторизированного доступа и повреждений (верно)**
	2. Доступны ли случайным лицам каталоги и внутренние телефонные книги, которые могут дать информацию о нахождении критичных ресурсов?	• Да • **Нет (верно)**
	3. Расположены ли ключевые информационные системы так, чтобы исключить случайный доступ к ним неавторизированным лиц?	• **Да (верно)** • Нет
Управление коммуникациями и операциями	1. Осуществляется ли распределение обязанностей как средство снижения риска от случайных и преднамеренных угроз?	• **Да, если критичные операции выполняются, как минимум, двумя сотрудниками или существует возможность сговора сотрудников с целью нанесения ущерба организации (верно)** • Нет
	2. Осуществляется ли оценка возможного риска и ущерба и занесение в контракт мер защиты, согласованных с подрядчиком, при привлечении сторонних организаций к управлению информационной системой?	• **Да (верно)** • Нет
	3. Закреплен ли документально процесс выполнения операций, определенных политикой безопасности?	• **Да (верно)** • Нет

Окончание таблицы Б.1

Управление доступом	1. Отражаются ли в политике контроля доступа правила и права каждой группы пользователей?	• Да • **Нет (верно)**
	2. Учитывает ли политика контроля доступа требования по безопасности отдельных бизнес-приложений и идентификацию всей информации, связанной с ними?	• **Да (верно)** • Нет
	3. Соблюдается ли соответствие между политикой управления доступом и классификацией информации различных систем и сетей?	• **Да (верно)** • Нет
Приобретение, разработка и поддержка систем	1. Определена ли ответственность для всего персонала, вовлеченного в процесс обработки и ввода исходных данных?	• **Да (верно)** • Нет
	2. Проводится ли проверка того, что программы запускаются в соответствующем режиме и останавливаются в случае неисправностей, а также, что связанные процессы останавливаются до устранения всех проблем?	• **Да (верно)** • Нет
	3. Проводится ли периодическая проверка целостности и правильности содержимого ключевых полей или файлов данных?	• **Да (верно)** • Нет
Управление бесперебойной работой организации	1. Сформулирована и задокументирована ли стратегия непрерывности ведения бизнеса, согласующая с установленными целями и приоритетами бизнеса?	• **Да (верно)** • Нет
	2. Определен ли четкий порядок внедрения контраварийных процедур для восстановления бизнес-процессов за требуемый промежуток времени?	• **Да (верно)** • Нет
	3. Является ли частью процесса обеспечения непрерывности ведения бизнеса соответствующая уровню рисков форма страхования?	• **Да (верно)** • Нет
Соответствие нормативным требованиям	1. Возможно ли превышение максимального числа пользователей в лицензии при использовании программного обеспечения?	• Да • **Нет (верно)**
	2. Соответствует ли законодательству порядок обращения с информацией о персональных данных сотрудников и клиентов?	• **Да (верно)** • Нет
	3. Разработаны ли в компании типовые процедуры приобретения программного обеспечения?	• **Да (верно)** • Нет