Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Амурский государственный университет»

Институт компьютерных и инженерных наук

Кафедра информационной безопасности

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ И ЗАЩИТЕ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ БАКАЛАВРА

для обучающихся направления подготовки

10.03.01 – «Информационная безопасность»

Благовещенск
2025

Бушманов А.В., Никифорова Л.В., Остапенко А.А, Самохвалова С.Г.

Методические указания к выполнению и защите выпускной квалификационной работы бакалавра для направления подгот.- Информационная безопасность / [ред. С.Г. Самохвалова]. – Благовещенск : АмГУ, 2025. – 43 с.

Настоящие методические указания предназначены руководителям выпускных квалификационных работ, студентам и выпускникам кафедры «Информационная безопасность» федерального государственного бюджетного образовательного учреждения высшего образования "Амурский государственный университет". В представленном материале обозначены требования к выполнению и защите выпускной квалификационной работе, по порядку и срокам выполнения работ, их защите, а также критерии их оценки.

Содержание

Введение

Целью итоговой аттестации является установление уровня подготовки выпускника к выполнению профессиональных задач и соответствия его подготовки требованиям федерального государственного образовательного стандарта высшего образования по направлению 10.03.01 «Информационная безопасность» (далее – ФГОС ВО).

В соответствии с ФГОС ВО к видам государственной итоговой аттестации (далее – ГИА) выпускников высшего учебного заведения относится – защита выпускной квалификационной работы (далее – ВКР).

ВКР дает возможность оценить уровень сформированности компетенций, изложенных в ФГОС ВО, профессиональные знания выпускников, их умения и навыки по осуществлению практической и/или научной деятельности.

ВКР может иметь теоретический, прикладной, теоретико–прикладной и творческий характер и должна отражать в себе научно–теоретические или научно–методические аспекты направления подготовки.

ВКР может выполняться студентом непосредственно на базе университета или, в случае соответствия нормам, на производственных базах предприятий, организаций и учреждений.

К защите ВКР допускается лицо, успешно завершившее в полном объеме освоение основной образовательной программы по направлению подготовки в соответствии с учебным планом. При условии успешного прохождения ГИА, выпускнику присваивается степень бакалавра и выдается диплом государственного образца о высшем образовании.

Лицам, не проходившим ГИА по уважительной причине (по медицинским показаниям или в других исключительных случаях, документально подтвержденных), должна быть предоставлена возможность пройти ГИА без отчисления из университета.

1 Цели и задачи ВКР

При выполнении ВКР студентам необходимо показать свою способность и умение самостоятельно решать актуальные задачи в области информационной безопасности, достаточно аргументировать и отстаивать свою точку зрения в ее решении.

Целью ВКР является закрепление и углубление теоретических знаний по информационной безопасности и защите информации, программно–техническим, организационным и правовым методам обеспечения информационной безопасности, приобретение практических профессиональных навыков и компетенций, опыта самостоятельной профессиональной деятельности.

Задачами выполнения ВКР являются:

самостоятельное исследование актуальных вопросов профессиональной деятельности;

изучение и использование современных информационных технологий в решении профессиональных задач;

систематизация, закрепление и расширение теоретических знаний по специальным дисциплинам;

углубление навыков ведения студентом самостоятельной исследовательской работы, работы с различной справочной и специальной литературой;

овладение методикой исследования при решении разрабатываемых в работе проблем.

Качество выполнения ВКР определяется тем, насколько студент овладел навыками сбора исходной информации, ее обработки, анализа, а также формулировки научно–обоснованных выводов, содержащихся в предлагаемых решениях.

ВКР свидетельствует об умении студентов:

четко формулировать тему исследования;

определять степень актуальности поставленной темы на современном

уровне;

собирать и анализировать исходные факты и материалы;

разрабатывать (или выбирать) методы исследования и проводить на их основе самостоятельное исследование;

делать обоснованные выводы, формулировать научные результаты и практические рекомендации по проделанной работе;

грамотно излагать свои мысли и результаты исследования;

правильно оформлять ВКР.

2 Организация процесса выполнения ВКР

Выпускная работа есть научное исследование, которое основано на глубоком изучении источников, научной литературы (монографий, статей, учебников, учебных пособий), собранном фактическом материале по избранной теме и обобщает учебно–исследовательскую и научно–исследовательскую работу студента за весь период обучения в университете.

ВКР должна содержать исследование актуальных проблем и вопросов комплексной защиты информации в разрезе их исторического, теоретического и практического развития и решения.

ВКР бакалавра – самостоятельное логически завершенное теоретическое и(или) экспериментальное исследование и прикладная разработка на заданную тему, подтверждающее умение обучающегося работать литературой, обобщать и анализировать фактический материал, используя теоретические знания и практические навыки, полученные при освоении образовательной программы бакалавра.

Примерная **тематика ВКР** разрабатывается выпускающей кафедрой, периодически обновляется. Студентам предоставляется право выбора примерной темы ВКР. Студент может предложить для ВКР тему, не вошедшую в примерную тематику, с необходимым обоснованием целесообразности ее разработки.

Тематика ВКР может включать решение следующих основных задач:

разработка специальных программных защитных средств;

разработка проектов использования имеющихся средств для защиты выбранного объекта;

разработка комплексной системы защиты информации предприятия, его отдельных помещений;

разработка методов анализа эффективности использования различных видов защиты информации на объектах защиты;

разработка требований, нормативно–правовой базы, процедур по обеспечению безопасности объектов;

исследование методов обеспечения надежной защиты объектов информатизации;

автоматизация процессов обеспечения безопасности объектов.

Выделяют типы ВКР:

Тип Т (теоретический) – работа, ориентированная на построение математических моделей процессов, возникающих при защите информации**.**

Тип ПТ (программно–технический) – работа, ориентированная на разработку аппаратуры и поддерживающего ее программного обеспечения, создаваемых с целью защиты информации, хранящейся в ЭВМ, системах и компьютерных сетях.

Тип С (сетевой) – работа, ориентированная на разработку защиты вычислительных сетей.

Тип П (программный) – работа, ориентированная на разработку средств системного и прикладного программного обеспечения, создаваемых с целью защиты информации, хранящейся в ЭВМ, системах и компьютерных сетях, аудита состояния компьютерных сетей, автоматизации процессов, связанных с аудитом безопасности, использования информационных технологий в образовательном процессе на курсах (предметах) по ИБ.

При выборе темы ВКР целесообразно учитывать:

интерес к решаемой проблеме;

актуальность проблемы;

степень разработки и освещенности исследуемой проблемы в литературе;

наличие у студента достаточного задела в данной области;

возможность получения необходимых данных для выполнения ВКР;

возможность получения конкретных практических результатов;

способности студента, уровень его теоретической и практической подготовки.

Целесообразно выбирать темы ВКР, которые удовлетворяют следующим условиям:

тема рекомендована потенциальными работодателями – стратегическими партнерами Университета, ведущими предприятиями, организациями, органами государственной власти;

тема отражает актуальные аспекты развития науки, техники и технологий и организации их использования в Амурской области, Российской Федерации;

тема соответствует разделу плана научно–исследовательской работы, проводимой кафедрой;

тема посвящена разработке (созданию) учебно–методического обеспечения работы кафедры;

отдельные аспекты темы прошли различные формы апробации.

Студент при выборе темы ВКР может использовать ранее выполненные работы в рамках научно–исследовательских, практических и курсовых работ, развивая и дополняя их, исходя из требований к выполнению ВКР.

Студент может предложить свою формулировку темы работы, если она соответствует требованиям направления подготовки, по которому он обучается.

Название темы ВКР должно отражать основную задачу работы, содержать наиболее существенные признаки проводимого исследования, быть по возмож-

ности кратким, емким и понятным. При формулировании темы ВКР, желательно избегать использования аббревиатур, сокращений и специальных терминов.

Как правило, название темы, начинается словами, определяющими характер работы как процесса: «Исследование…», «Анализ…», «Разработка…». Далее кратко характеризуется суть самой работы.

Ориентировочный перечень рекомендуемых тем ВКР приведён в приложении 1 и может ежегодно корректироваться.

Предварительная формулировка темы обсуждается и корректируется с руководителем ВКР и согласуется с заведующим выпускающей кафедрой.

После выбора темы студент на имя заведующего кафедрой до 20 ноября текущего года пишет заявление с просьбой об утверждении выбранной им темы ВКР (приложение 2).

Выпускающая кафедра утверждает перечень тем ВКР, предлагаемых студентам, и доводит его до сведения студентов не позднее, чем за 6 месяцев до даты начала ГИА.

Для подготовки ВКР за студентами приказом ректора закрепляется руководитель ВКР из числа преподавателей выпускающей кафедры. Для выполнения некоторых разделов ВКР может назначаться консультант.

Если в процессе выполнения ВКР выясняется необходимость изменения формулировки темы работы, то по согласованию с руководителем ВКР и заведующим выпускающей кафедрой возможна корректировка выбранной темы, но не позднее, чем за две недели до защиты. Новая тема утверждается приказом ректора по университету.

3 Требования к структуре и содержанию ВКР

Пояснительная записка бакалаврской работы включает в себя:

титульный лист;

бланк «задание»;

реферат;

нормативные ссылки;

перечень обозначений и сокращений;

содержание**;**

введение;

основную часть, состоящую, как правило, не менее чем из трех разделов;

заключение, включающее выводы и предложения (рекомендации) по внедрению и использованию результатов ВКР;

библиографический список;

приложения (при необходимости).

3.1 Титульный лист

На титульном листе номер страницы не проставляется, но он включается в общую нумерацию страниц пояснительной записки.

Титульный лист оформляется в соответствии с приложением 3 и должен быть оформлен в текстовом редакторе.

3.2 Задание

Задание оформляется на стандартном бланке, получаемом на выпускающей кафедре. Образец бланка «задание» приведен в приложении 4.

Текст задания подписывается научным руководителем и студентом, утверждается заведующим выпускающей кафедрой.

3.3 Реферат

Текст реферата содержит краткие сведения о ВКР, помогающие понять смысл описываемой в дальнейшем работы.

Реферат включает в себя следующую информацию:

сведения об объеме ВКР, количестве иллюстраций, таблиц, приложений и использованных источников;

перечень ключевых слов или словосочетаний (от 5 до 15), в наибольшей мере характеризующих содержание пояснительной записки. Ключевые слова

записываются в именительном падеже и оформляются прописными буквами в единую строку перечислением через запятую;

текст объемом не более 20 строк, отражающий суть объекта исследования или разработки, цель работы, использованные методы, полученные результаты, информацию об использовании данной работы, область применения.

Пример оформления реферата приведен в приложении 5.

3.4 Нормативные ссылки

Среди используемых в процессе работы литературных источников существует тип изданий – стандарты, регламентирующие ряд наиболее значимых вопросов в сфере информационной безопасности и определяющие уровни защиты информации и соответствующие им требования к содержанию базового состава мер защиты информации.

Использованные в ВКР стандарты должны быть указаны в виде перечня нормативных ссылок. Пример оформления нормативных ссылок и перечень наиболее часто используемых в работе над ВКР по данным направлениям подготовки, приведен в приложении 6.

3.5 Определения, обозначения и сокращения

Изложение сути работы должно быть построено логично и построено так, чтобы любой человек, читая текст ВКР, максимально точно и однозначно воспринимал все используемые в нем понятия. Используемая терминология должна быть общепринятой в рассматриваемой предметной области. Как правило, терминология регламентирована соответствующими ГОСТами, в которых для каждого термина приводится его точное определение, а также обозначение или сокращение. Кроме ГОСТа, общепринятую терминологию каждой предметной области определяют различные словари, справочники и отраслевые нормативные документы.

Использование сокращений и условных обозначений значительно облегчает текст ВКР, делая его более компактным и удобочитаемым.

Помимо таких общеизвестных сокращений, как АС, БД, ЭВМ и других, разрешается вводить собственные сокращения, отражающие наиболее часто повторяющиеся термины. Для их ввода требуется дать их расшифровку непосредственно при первом упоминании в тексте ВКР (например, «...особое место в области информационной безопасности (ИБ) уделяется ...»).

Все малораспространенные сокращения, встречающиеся в тексте более двух раз, должны быть сведены в отдельный перечень сокращений.

Пример составления и оформления перечня обозначений и сокращений приведен в приложении 7.

3.6 Содержание

В содержании должны быть перечислены все смысловые элементы ВКР: введение, заключение, структурные элементы основной части (разделы, подразделы, пункты), библиографический список и приложения.

Названия элементов содержания должны полностью совпадать с названиями, приведенными в тексте ВКР с использованием шрифта основного текста без курсивного и полужирного выделения.

Пример оформления содержания приведен в приложении 8.

3.7 Введение

Во введении излагаются общие сведения по тематике разработки или исследования, определяется актуальность выбранного направления, кратко отмечаются проблемные вопросы, степень их решения в конкретной предметной области. Рассматриваются новые возможности на базе применения современных защитных средств, обеспечивающих информационную безопасность исследуемых объектов. Введение завершается четкой формулировкой цели выполняемой работы и перечислением основных решаемых задач.

Объем введения составляет, как правило, не более трех страниц текста.

3.8 Основная часть

В зависимости от специфики работы число разделов основной части, их

конкретные названия могут меняться. В виде самостоятельных разделов могут быть приведены расчеты экономической эффективности и/или надежности, вопросы информационной безопасности, безопасности жизнедеятельности.

3.8.1. Раздел «Теоретические основы изучаемой проблемы»

Теоретическая часть исследования должна быть ориентирована на разработку теоретических и методологических основ изучаемых объектов (процессов, материалов и др.), использование новых концепций и идей в выбранной области, отличаться определенной новизной научных идей и методов исследований.

Задачами теоретической части являются раскрытие понятий и сущности изучаемых явлений или процессов и обоснование на этой основе мер и методов по обеспечению защиты информации выбранного объекта.

В теоретической части на основе обзора отечественной и зарубежной литературы, достижений в области информатизации и по другим источникам обосновывается выбор применяемых методов, описывается их суть, принципы их использования. Здесь также возможно рассмотреть тенденции развития тех или иных социальных, экономических, информационных процессов на предприятии в результате реализации предлагаемых решений.

Для задач, решаемых на основе программно–аппаратной защиты информации объектов, необходимо рассмотреть модели компьютерных систем, модели безопасного взаимодействия и управления безопасностью в информационных системах, модели сетевых средств безопасности, методы декомпозиции моделей угроз, обосновать выбор методов и средств защиты информации выбранного объекта на аппаратном и/или программном уровнях.

Для задач, связанных с защитой и обработкой конфиденциальных документов, необходимо рассмотреть типовой состав технологических стадий входного, выходного и внутреннего документопотоков, провести анализ несанкционированного получения документированной информации, каналов практиче-

ской реализации возможных угроз, принципов защиты документопотоков, обосновать выбор защищенной технологии и уровень ее автоматизации.

Для задач, решаемых с правовым обеспечением защиты информации на предприятиях, в телекоммуникационных и информационных сетях, организациях, а также информации, составляющую государственную, коммерческую и другие тайны, интеллектуальную собственность, должны быть рассмотрены и проанализированы соответствующие законодательные акты, виды, условия и порядок их применения. Должен быть выбран и обоснован комплекс правовых мер и мероприятий, обеспечивающих защиту выбранного объекта.

Для задач, решаемых на основе инженерно–технической защиты информации выбранного объекта, необходимо провести анализ существующих методов, способов и средств его инженерно–технической охраны в соответствии с видами угроз, основ организации и методического обеспечения такой защиты, выбрать и обосновать комплекс организационно–распорядительных мероприятий по защите объекта.

Для задач, решаемых с использованием криптографических систем защиты объектов, необходимо обосновать выбор криптосистем, требования к ним, характеристики, режимы их применения, определить алгоритмы их реализации в виде блок–схем или пошагового описания, соответствующего языка программирования, рассмотреть модели таких систем с позиций надежности защиты и экономики.

Для задач, решаемых на основе применения организационных мер по защите информации выбранного объекта, необходимо рассмотреть совокупность нормативных и распорядительных документов, определяющих политику информационной безопасности объектов, обладающих конфиденциальной информацией, принципы и задачи ограничения и разграничения доступа к такого рода информации, обосновать необходимость применения такого рода мер, разработать модель их использования.

Для решения задач комплексной защиты информации на предприятии должен быть проведен системный анализ основ защиты информации, должны быть рассмотрены модели комплексной системы защиты информации (КСЗИ): функциональная, информационная, организационная, потенциального нарушителя, на основе которых может быть определен технический и/или рабочий проект организации КСЗИ с технико–экономическим обоснованием. Указанное обоснование необходимо представить в виде аналитического описания или в виде алгоритмической интерпретации. Могут быть описаны средства, обеспечивающие функционирование КСЗИ с учетом различных ситуаций.

На основе теорий различных дисциплин в этом разделе должны быть в рамках ВКР достаточно подробно описаны алгоритмы, модели, методы, способы, меры, которые после рассмотрения различных альтернатив в конечном итоге должны быть положены в базовую часть проектной части работы.

В теоретической части студент имеет право сделать собственные предложения по развитию, совершенствованию, модернизации, адаптации математических моделей, алгоритмов, аналитических выражений к особенностям рассматриваемых задач, может предложить собственные концепции решения задач, собственные подходы к тем или иным аспектам проблематики.

Теоретическая часть должна заканчиваться выводами по рассмотренным вопросам с обоснованием решений по главным направлениям работы.

Объем теоретической части ВКР может составлять 20–30 страниц. Для ВКР, которая, носит исследовательский характер, объем теоретической части по согласованию с руководителем может быть увеличен до 50 страниц за счет сокращения объемов других разделов.

3.8.2. Раздел «Проектная часть изучаемой проблемы»

Задачей проектной части ВКР является реализация и описание предложенных студентом разработок в рамках выбранной темы и с учетом специфики конкретного объекта и аспектов исследования, подходов, методов и средств ре-

шения конкретных задач.

В рамках разработок могут включаться задачи совершенствования (улучшения) существующих систем обеспечения безопасности выбранного объекта. При этом на основе принятых проектных предложений следует определить и указать в работе имеющиеся системы защиты информации, указать их конкретную конфигурацию, схему применения и дополнить предложенными дипломником комплексом мер, улучшающим безопасность объекта.

Проектная часть должна содержать материал соответствующий исключительно конкретным особенностям объекта и задачам разработки. Здесь должны быть реализован технический и/или рабочий проект. В соответствии с поставленными задачами могут быть представлены:

модели безопасности объектов;

алгоритмы решения поставленных задач по защите выбранного объекта;

схемы алгоритмов основных программных модулей, их взаимосвязи и описания;

программные модули, их взаимосвязи и описания;

информационные модели защищаемой информации;

комплексы инженерно–технических средств по обеспечению безопасности объекта;

структуры аппаратных защитных средств;

шифровальные средства и их ключи;

правовые меры, ориентированные на защиту выбранного объекта;

организационные меры по защите исследуемого объекта;

комплекс организационно–технических мероприятий по внедрению предложенных в ВКР решений.

При описании информационных моделей необходимо подробно осветить в них организацию данных, рассмотрев следующие вопросы:

обоснование принятых форм хранения данных в памяти компьютера (база

данных или совокупность файлов);

обоснование выбора модели логической структуры базы данных;

обоснование выбора СУБД;

обоснование методов организации файлов;

использование диалога.

Проектную часть желательно закончить кратким перечнем основных предложенных в работе проектных решений.

Примерный объем проектной части составляет 20–30 страниц.

3.8.3 Вопросы экономической эффективности результатов работы

В ВКР может быть дана оценка эффективности внедрения на предприятии проектных предложений по обеспечению информационной безопасности объектов защиты. Возможны различные подходы к ее определению:

сравнение вариантов существовавшей системы безопасности объекта (ов) защиты и разработанной дипломником с расстановкой акцентов на ее преимуществах. При использовании такого подхода необходимо приложение справки от предприятия о внедрении разработки;

расчет количественных характеристик экономической эффективности, определяемой из соотношений между гипотетическими доходами, измеряемыми возможными потерями из–за отсутствия надежной системы безопасности на объектах защиты, и произведенными затратами на внедрение предложенной системы.

3.8.4 Вопросы безопасности жизнедеятельности

В данном разделе необходимо обосновать все решения, связанные с организацией взаимодействия человека с созданным вами программным продуктом. Для общей оценки человеко–машинного интерфейса необходимо:

оценить его воздействие на здоровье работающего человека (выработка рекомендаций к техническим характеристикам монитора, режиму труда и отдыха, прогнозирование степени загруженности человека);

выполнить анализ условий эксплуатации рабочего места, сформулировать требования к факторам внешней среды – освещенности, микроклимату и др.;

обосновать общую компоновку информации на экране компьютера или панели устройства, включая оценку относительной значимости элементов композиции;

обосновать выбор цветовой и шрифтовой палитры, включая освещение вопросов привлечения внимания и функциональное назначение различных цветов и шрифтов;

оценить простоту работы созданного программного продукта, интуитивную понятность интерфейса для неподготовленного пользователя, качество эксплуатационной документации, необходимость обучения пользователя;

провести анализ логической сложности работы пользователя, оптимальность созданной системы меню, обосновать необходимость выдачи пользователю той или иной информации;

спрогнозировать возможные ошибки пользователя и предусмотреть в системе защиту от них.

Не все из перечисленных вопросов должны обязательно освещаться в каждой ВКР – все зависит от специфики ВКР.

3.9 Заключение

Заключение должно содержать только те выводы, которые согласуются с целью исследования, сформулированной в разделе «Введение» и должны быть изложены таким образом, чтобы их содержание было понятно без чтения текста работы. В заключении следует перечислить наиболее значимые результатов работы, которые необходимо сопроводить комментариями или выводами. Заключение должно быть четким, понятным и желательно, чтобы оно умещалось на одной странице.

Как правило, заключение начинается фразой: «При выполнении ВКР были выполнены следующие этапы:…» и приводятся решенные задачи с особен-

ностями их выполнения.

3.10 Библиографический список

Библиографический список является важнейшим компонентом ВКР и предназначен для документального подтверждения интерпретируемого или цитируемого материала, а также для отражения эрудиции автора ВКР, степени его знакомства с актуальной литературой в рассматриваемой предметной области. Список должен содержат перечень 25 – 30 литературных источников, материал которых был использован при создании ВКР. Особое внимание должно быть уделено изданиям последних лет. В них наиболее полно отражены современный подход к решению поставленной проблемы и практическое его применение, показаны новые и прогрессивные взгляды, которые следует использовать при изложении основных вопросов избранной темы.

На все источники из списка должны быть ссылки в тексте ВКР.

3.11 Приложения

В приложения рекомендуется выносить вспомогательный материал, дополняющий текст ВКР, но не влияющий непосредственно на его восприятие и понимание. В этом разделе приводятся расчетные, графические материалы (при значительном объеме вычислительных работ по ВКР); формы документов, отражающих анализ производства и управления; рабочая проектная документация (положения, должностные инструкции, формы документов и т.д.), а также другие материалы, использование которых в тексте пояснительной записки перегружают ее и нарушает логическую стройность изложения.

Также в качестве приложений в состав пояснительной записки входят дополнительные материалы исследований, отчеты о публикациях и представлении результатов работы на различных мероприятиях, свидетельства о регистрации, тексты лицензионных соглашений, исходные материалы исследований, отрывки программного кода, сертификаты и справки, рецензии, отзывы, характеристики и другие документы и данные, детализирующие, обосновывающие и поясняю-

щие текст пояснительной записки и сделанных в ней выводов.

Приложения располагаются в конце ВКР в порядке появления соответствующих ссылок в тексте.

Каждое приложение должно иметь собственный заголовок (название), который отражает содержание этого приложения.

4 Подготовка ВКР к защите

4.1 Требования к объему текста ВКР

Объем бакалаврской работы составляет, как правило, 50–70 страниц. Приложения в указанный объем бакалаврской работы не включаются.

Основная часть, как правило, должна занимать около 70–80% от общего объема работы. Например, при объеме пояснительной записки в 60 страниц, около 45 страниц должна занимать основная часть, до 15 страниц – остальные структурные элементы. При этом из них не менее 30 страниц должны быть посвящены непосредственно проектной части работы и полученным результатам. При большом количестве таблиц и рисунков их следует вынести в приложения. Объем приложений не регламентируется.

ВКР оформляется в соответствии с локальными нормативными документами университета.

4.2 Стиль изложения

Текст ВКР не должен содержать грамматических и орфографических ошибок. Автор должен использовать грамотный литературный стиль изложения, демонстрируя правильное применение специализированной терминологии. Полуграмотный и косноязычный текст – не более чем проявление лени и некультурности.

Применяемый стиль изложения – безличный. Он подразумевает использование вместо фраз «мною сделано» или «нами получены» конструкций типа «было сделано или «в ходе работы получены».

Используемый материал должен быть максимально сжат, из него исключено лишнее, сомнительное и несущественное. Требуется проявлять осторожность при заимствовании текстов из литературных источников и сети Интернет. Необходимо помнить, что материал работы должен быть авторским и проверен на отсутствие плагиата (итоговая оценка оригинальности ВКР обучающихся, должна составлять не менее 50% – для ВКР (бакалаврская работа).

Материал должен быть логично сгруппирован, информация должна приводиться именно там, где она необходима для понимания смысла. Нужно избегать длинных предложений и неоднозначных формулировок.

Нужно стараться максимально просто и понятно излагать материал. Последствием плохого языка может стать непонимание или неправильное толкование излагаемого материала.

При выражении логических связей между частями высказывания следует использовать указательные местоимения «этот», «тот», «такой» (например, «эти данные можно использовать для вывода...»). Местоимения «что – то», «кое – что», «что–нибудь» в силу неопределенности их значения в тексте работ не используются.

Важнейшим средством выражения логических связей являются специальные синтаксические средства, указывающие:

последовательность развития мысли (прежде всего, в первую очередь, одновременно, в то же время, предварительно, ранее, во – первых и др.);

противоречивые отношения (однако, но, так же, как и..., не только, но и..., по сравнению, в отличие, в противоположность, наоборот и др.);

причинно – следственные отношения (поэтому, потому, так как, поскольку, отсюда следует, откуда следует, вследствие, в результате и др.);

дополнения или уточнения (причем, при этом, вместе с тем, кроме того, более того, главным образом, особенно и др.);

переход от одной мысли к другой (прежде чем перейти к ..., обратимся к

..., рассмотрим, необходимо рассмотреть и др.);

при ссылки на предыдущее или последующее высказывание (как было сказано, как говорилось выше, согласно этому и др.);

вывод (таким образом, итак, следовательно, в результате, в итоге, в конечном счете, отсюда , подводя итог, следует сказать... и др.);

ввод новой информации (рассмотрим следующие случаи, остановимся подробно на..., приведем несколько примеров, основные преимущества этого метода..., несколько слов о перспективах исследования и др.).

Не допустимо использование жаргона, особенно профессионального. Неграмотным является использование слов типа «винт», «скриншот», «кликнуть», «ибешник» и т.п. Опытные специалисты очень скрупулезно следят за своим языком, используя правильно каждый термин при создании технической и научной документации. Помните, что наиболее надежными источниками терминов являются ГОСТ, справочники, словари, учебники и научные издания.

4.3 Промежуточный контроль готовности ВКР

В целях контроля и осуществления успешной планомерной работы над ВКР студент должен регулярно информировать руководителя о ходе ее выполнения и согласовывать с ним свои дальнейшие действия, руководитель и студент должны встречаться для консультаций, как правило, не реже одного раза в неделю.

Подготовленная пояснительная записка ВКР проходит проверку на Антиплагиат и Нормоконтроль на выпускающей кафедре за две недели до защиты. Успешное прохождение «Нормоконтроль» визируется на титульном листе. Затем работа переплетается (брошюруется) автором.

Полностью переплетенная ВКР предоставляется на отзыв руководителю не позднее, чем за неделю до начала ГИА. Затем вместе с отзывом сдается заведующему выпускающей кафедрой для получения допуска к защите.

Заведующему кафедрой также предоставляется справка о внедрении ре-

зультатов работы, если таковая имеется в наличии, и результат проверки на плагиат.

4.4 График проведения защит ВКР

Обычно в апреле – мае текущего года утверждается состав государственной экзаменационной комиссии (далее – ГЭК) и назначаются даты защиты ВКР (как правило, период с 20 по 30 июня текущего года).

Расписание защит ВКР и график защит в конкретный день составляется заведующим выпускающей кафедрой и доводится до сведения студентов через информационный стенд не позднее, чем за 10 дней до начала ГИА.

4.5 Предварительная защита квалификационных работ

С целью оказания помощи студентам в подготовке к защите ВКР кафедрой может быть организована предварительная их защита. Ее цель – оценить готовность работы и студента к защите, объем и качество оформления представляемого материала. Предварительная защита назначается обычно за 15–20 дней до защиты ВКР, график проведения доводится до студентов. Для проведения предварительной защиты формируются комиссии, состоящие из ведущих преподавателей выпускающей кафедры.

На предварительную защиту представляются полностью оформленная, но не сброшюрованная пояснительная записка с подписями студента и руководителя на титульном листе и компьютерная презентация.

4.6 Допуск и подготовка к защите

В установленные сроки (обычно за 5 дней до защиты) выпускник предоставляет заведующему выпускающей кафедрой для рассмотрения и допуска к защите законченные материалы ВКР, которые включают:

переплетенную и подписанную выпускником и руководителем пояснительную записку;

протокол проверки на плагиат, подписанный руководителем ВКР;

отзыв руководителя;

электронный носитель с ВКР (компакт–диск или флэш–накопитель).

После ознакомления с материалами ВКР заведующий кафедрой принимает решение о допуске студента к защите. Допуск подтверждается резолюцией на титульном листе пояснительной записки.

4.7 Требования к оформлению презентации

В ходе защиты выпускник должен за короткое время довести до членов ГЭК большой объем информации.

За 5–7 минут члены ГЭК должны не только вникнуть в предметную область, понять смысл работы, ее цель, но и оценить уровень выполнения ВКР и степень значимости полученных результатов. Чтобы упростить восприятие работы, более четко структурировать ее изложение, сделать результаты более наглядными и убедительными, доклад необходимо сопровождать компьютерной презентацией.

Объем презентации – не более 17 слайдов. Подавляющая часть материала – формулы, рисунки, схемы, графики. Количество текста необходимо минимизировать, приводить его в тезисном варианте. На первом слайде указывается тема работы, ФИО автора и руководителя, второй слайд посвящен целям, задачам, практической значимости работы. На последнем – приводится краткое изложение заключения ВКР. Остальные слайды посвящены этапам выполнения работы в порядке, представленном в работе и докладе.

Возможно включение в презентацию видео, демонстрирующего работу созданного ПО, но его продолжительность не должна превышать 30 секунд.

Если презентация содержит формулы, их необходимо пронумеровать.

Слайды также необходимо сопроводить нумерацией.

Рекомендуется согласовать содержимое презентации с руководителем ВКР.

Установка презентаций проходит за один день до защиты работы, проверяется ее соответствие используемому в аудитории ПО, необходимому для ее

воспроизведения.

4.8 Требования к докладу

В докладе необходимо изложить актуальность и обоснованность темы, раскрыть основное содержание ВКР, отметить оригинальные решения и дать им обоснование. Общеизвестные положения и сведения в докладе излагать не рекомендуется. При защите ВКР рекомендуется руководствоваться планом или тезисами доклада.

Не уменьшайте значимость доклада. Недостаточная его подготовка может свести на нет даже превосходную работу. Можно сказать, что хороший доклад на 80 % гарантирует успешную защиту, конечно, при условии, что студент уверенно отвечает на вопросы комиссии.

Основные признаки плохого доклада:

слабое владение темой ВКР и/или рассматриваемой предметной областью;

не готовность к эмоциональному напряжению, которое, как правило, сопровождает процедуру защиты;

отсутствие опыта публичных выступлений, что проявляется в неконтролируемых сознанием докладчика, а потому незаметных для него ненужных, а иногда и некрасивых действиях (почесывание, болтание указкой из стороны в сторону, держание руки в кармане и прочему).

Текст доклада нужно заранее проработать и желательно выучить. Из–за присутствующего волнения, нужные слова могут забываться, возникать неприятные паузы в ходе доклада, что существенно снижает его качество и формирует негативное мнение комиссии обо всей работе.

Но худший вариант доклада – чтение с листа.

Продолжительность доклада – 5–7 мин, приветствуется четкость изложения.

Традиционно, доклад представляют в следующей последовательности:

вступление (обращение к комиссии);

актуальность и проблемы, решаемые в работе;

цели и задачи работы, практическая или научная значимость;

основная часть;

заключение (выводы);

окончание доклада.

Вступление (обращение к комиссии) служит для обозначения начала доклада. Обычно оно звучит так: "Добрый день, уважаемые члены государственной экзаменационной комиссии!". Помимо проявления уважения к комиссии, обращение стимулирует ее членов прервать разговоры, записи и другие мелкие текущие дела, полностью сосредоточиться на Вашем докладе.

Название темы ВКР включать в доклад не следует, поскольку ее называет секретарь комиссии.

Если ВКР выполнена по заявке предприятия, надо обязательно доложить о внедрении результатов, подтверждаемых актом или справкой о внедрении.

Окончание доклада должно быть также четко обозначено, чтобы комиссия могла преступить к вопросам. Например, можно сказать: "Доклад закончен. Благодарю за внимание" и т.п.

При выступлении необходимо соблюдать следующие правила:

начинать доклад следует после объявления секретарем ГЭК темы ВКР и фамилии докладчика;

стоять надо всегда лицом к комиссии. Возможно, переключить свое внимание на некоторое время на экран с презентацией, навести на него указку, а затем вновь повернуться лицом к членам комиссии;

при показе на слайдах чертежей, схем, таблиц и т.д. ни в коем случае не следует махать указкой, не читать их содержание, а рассказывать выводы, следующие из их просмотра;

нельзя отвлекаться на посторонние раздражители (вход в аудиторию по-

сторонних, перемещение одного из членов комиссии и т.п.) и прерывать из–за них свою речь.

Готовя доклад, не забывайте, что, к сожалению, наиболее часто задаваемым вопросом является: «Ваш личный вклад в работе?» Постарайтесь, чтобы он был раскрыт в докладе.

4.9 Требования к внешнему виду защищающегося

На защите студент должен придерживаться офисного стиля в одежде. Если защита проходит в жаркий день, допустимо отсутствие пиджака и длинного рукава рубашки. В целом, форма одежды должна подчеркивать уважение докладчика к комиссии и торжественность момента. *В одежде не допускаются шлепанцы, шорты, майки, футболки*, излишне короткие юбки*, топы.*

4.10 Необходимые действия перед процедурой защиты

За день до защиты выпускник должен установить свою презентацию на компьютер в аудиторию, в которой назначена защита. Проверка работоспособности презентации обязательна.

При использовании дополнительных программных продуктов или разработок, планируемых к демонстрации, также необходимо убедиться и в их работоспособности.

Необходимо сдать материалы ВКР (электронный и бумажный вариант) и полный комплект сопроводительных документов (отзыв руководителя, протокол проверки на плагиат, акт об использовании работы, распечатка презентации) секретарю ГЭК не позднее, чем за один день до защиты.

4.11 Процедура защиты квалификационных работ

Защита ВКР проходит на открытом заседании ГЭК. Возглавляет ГЭК председатель, кандидатура которого ежегодно утверждается Министерством науки и высшего образования РФ.

Председатель ГЭК утверждается из числа лиц, не работающих в университете, имеющих ученую степень доктора наук и (или) ученое звание профессо-

ра либо являющихся ведущими специалистами – представителями работодателей или их объединений в соответствующей области профессиональной деятельности.

Членами ГЭК являются ведущие преподаватели выпускающей кафедры и специалисты профильных предприятий.

Обучающимся и лицам, привлекаемым к ГИА, во время ее проведения запрещается иметь при себе и использовать средства связи.

Процедура защиты ВКР обычно проходит по следующему сценарию.

1. Секретарь ГЭК приглашает к защите выпускника, зачитывая его фамилию, имя, отчество и тему ВКР.

2. Председатель предоставляет студенту слово для доклада.

3. Студент излагает доклад, в котором освещается постановка задачи, существо работы и полученные результаты. Длительность доклада не должна превышать 7 минут для ВКР.

4. После окончания доклада председатель предлагает членам комиссии задать вопросы по представленной работе.

5. После окончания ответов на вопросы, зачитывается отзыв руководителя, а также прочие документы, представленные в ГЭК (например, акты о внедрении, отзывы о работе с предприятий).

6. Затем студенту предоставляется слово для ответов на замечания руководителя. Если замечания существенны, то необходимо четко, уверенно в краткой форме обосновать свою позицию. Если замечания несущественны, рекомендуется с ними согласиться.

7. После ответов на замечания защита объявляется законченной.

4.12 Ответы на вопросы

По окончанию доклада по предложению председателя члены ГЭК задают вопросы.

Как правило, вопросы непосредственно связаны с тематикой работы, од-

нако не исключаются и любые другие вопросы как теоретического, так и практического характера по всем дисциплинам, освоенной образовательной программы.

Также могут быть заданы вопросы, ответы на которые могут подтвердить (опровергнуть) профессиональную компетентность докладчика.

Вопросы задаются в устной форме и заносятся секретарем ГЭК в протокол.

Не следует торопиться с ответом на вопрос, не дослушав его до конца и не поняв его сути. Рекомендуется внимательно выслушать вопрос, если что–то непонятно – уточнить. Затем, одним – двумя предложениями четко и уверенно ответить.

В ответах на вопросы следует активно использовать материал, представленный на слайдах. Это касается, в том числе, и числовых данных, которые можно не знать на память.

Возможна ситуация, когда членом комиссии, задается вопрос о том, что уже сказано выпускником ранее или вопрос повторяет ранее заданный. Достаточно невежливым считается ответ: "Об этом уже сказано ранее" и т.п. Возможно, докладчик недостаточно точно или неоднозначно ответил. Следует повторить ответ, причем столько раз, сколько вопрос будет задан.

На вопросы, не связанные с представленной ВКР, можно просто ответить: "Этот вопрос в ВКР не рассматривался". Если же выпускник знает ответ на него, ответ лучше начать с оговорки: "Этот вопрос в ВКР не рассматривался, но" и т.д.

Самая сложная и неприятная ситуация возникает, если выпускник, не зная ответа на вопрос, просто молчит. Это вынуждает члена комиссии повторить вопрос, уточняя его. При этом недопустимо, чтобы «немая сцена» повторилась. Можно все же попытаться ответить наугад. Но если ответ совсем неизвестен, тогда прямо сказать: "Я затрудняюсь ответить".

4.13 Критерии оценки выпускных квалификационных работ

Оценка ВКР и решение о присвоении выпускнику соответствующей квалификации принимаются коллегиально на закрытом заседании ГЭК открытым голосованием.

ВКР сначала оценивается каждым членом комиссии согласно критериям оценки сформированности компетенций, предусмотренных соответствующими образовательными программами, а затем выставляется коллегиально.

Результаты защиты ВКР определяются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

При выставлении оценки по защите ВКР ГЭК **учитывает**:

качество выполнения ВКР и самостоятельность выпускника;

обоснованность принятых решений;

актуальность решаемых задач;

оригинальность принятых решений;

качество оформления и грамотность изложения материалов ВКР;

умение логично, четко, грамотно, выразительно представлять доклад;

убедительность ответов на вопросы и умение защищать выдвинутые в ВКР научно–технические и практические предложения.

Кроме того, при выставлении окончательной оценки по защите ВКР ГЭК **может учитывать**:

мнение руководителя;

средний балл за весь период обучения,

внедрение результатов ВКР,

наличие публикаций по теме исследования и др.

В спорных случаях решение принимается большинством голосов, присутствующих членов ГЭК, при равном числе голосов голос председателя является решающим.

Критерии оценки ВКР представлены в фонде оценочных средств ГИА по направлениям подготовки 10.03.01 – Информационная безопасность.

Оценки объявляются в день защиты ВКР после оформления в установленном порядке протокола заседания ГЭК. В протоколе отмечаются вопросы, заданные выпускнику, особые мнения членов ГЭК, оценка выполнения ВКР и его защиты. В нем также регистрируется запись о присуждении квалификации и определение степени диплома (например, с отличием), отмечается практическая ценность, рекомендации в магистратуру.

Наиболее, интересные как в теоретическом, так и практическом отношении ВКР могут быть рекомендованы к участию в конкурсе научных работ. Авторы таких работ могут быть рекомендованы для поступления в магистратуру. На заключительном этапе заседания председатель ГЭК в торжественной обстановке публично объявляет общие результаты и оценки защиты каждого студента, а также рекомендации по продолжению обучения.

После защиты экземпляр ВКР передается на кафедру, для хранения.

Список использованных источников

1. Федеральный закон Российской Федерации от 29 декабря 2012 г. №273–ФЗ "Об образовании в Российской Федерации".

2. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 – «Информационная безопасность (уровень бакалавриата)» (утвержден Приказом Министерством образования и науки РФ от 17 ноября 2020 г. № 1427).

3. Приказ Министерства образования и науки РФ от 29 июня 2015 г. № 636 «Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программа специалитета и программам магистратуры»,

4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф.– М.: ИД ФОРУМ, НИЦ ИНФРА–М, 2017. – 416 с.

5. Глинская Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. Пособие / Е.В. Глинская, Н.В. Чичварин. – М. : ИНФРА–М, 2018. – 118 с.

6. Партыка Т. Л. Информационная безопасность: учеб. Пособие / Т.Л. Партыка, И.И. Попов. – 5–е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА–М, 2018. – 432 с.

7. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. – М.: Форум: НИЦ ИНФРА–М, 2013. – 368 с.

8. Козырь Н. С. Экономические аспекты информационной безопасности: учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. – Москва: Издательство Юрайт, 2025. – 131 с.– ISBN 978–5–534–17863–0. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/568708.

9. Соловьев, Н. А. Выпускная квалификационная работа бакалавра. Методические указания: учебное пособие / Н. А. Соловьев, Т. В. Волкова, Л. А. Юркевская. – Санкт–Петербург: Лань, 2022. – 68 с. – ISBN 978–5–8114–3337–7. – Текст: электронный // Лань: электронно–библиотечная система. – URL: https://e.lanbook.com/book/206270

10. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. – Москва: Ай Пи Ар Медиа, 2021. – 83 с. – ISBN 978–5–4497–1164–9. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/108227.html

11. Проектирование информационных систем: учеб. Пособие / В.В. Коваленко. – М. : ФОРУМ : ИНФРА–М, 2018. 320 с.

12. Дронов, В. Ю. Бизнес–процесс «Обеспечение информационной безопасности организации»: учебное пособие / В. Ю. Дронов, Г. А. Дронова. – Новосибирск: Новосибирский государственный технический университет, 2021. – 76 с. – ISBN 978–5–7782–4537–2. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/126547.html

13. Баланов, А. Н. Комплексная информационная безопасность: полный справочник специалиста: практическое пособие / А. Н. Баланов. – Москва, Вологда: Инфра–Инженерия, 2024. – 156 с. – ISBN 978–5–9729–1771–6. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/143356.html

14. Дик Д. И. Дипломное проектирование: учебное пособие / Д. И. Дик. – Курган: КГУ, 2018. – 148 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/177905

15. Казарин О. В Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. – Москва: Издательство Юрайт, 2021. – 342 с.

Приложение 1

Примерный перечень ВКР

1. Организация безопасного удаленного доступа к ЛВС предприятия (название предприятия).
2. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии (название предприятия).
3. Автоматизация учета конфиденциальных документов на предприятии (название предприятия).
4. Организация процессов мониторинга конфиденциального документооборота на предприятии (название предприятия).
5. Автоматизация процесса проверок наличия конфиденциальных документов на предприятии (название предприятия).
6. Разработка комплексной системы защиты информации (КСЗИ) предприятия (название предприятия).
7. Организация системы планирования и контроля функционирования КСЗИ на предприятии (название предприятия).
8. Разработка основных направлений совершенствования КСЗИ предприятия (наименование предприятия).
9. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии (наименование предприятия).
10. Разработка методологии проектирования КСЗИ.
11. Разработка моделей процессов защиты информации при проектировании КСЗИ.
12. Анализ методов оценки качества функционирования КСЗИ.
13. Разработка структурно–функциональной модели управления КСЗИ предприятия (наименование предприятия).
14. Разработка проекта программно–аппаратной защиты информации предприятия (наименование предприятия).
15. Разработка игровой (дискретной) модели программно–аппаратной защиты информации предприятия (наименование предприятия).
16. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (название предприятия).
17. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет (название предприятия).
18. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями (название предприятия).
19. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации (название предприятия).
20. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (название предприятия).
21. Использование институтов правовой защиты интеллектуальной собственности для защиты информации (название объекта).
22. Организация защиты персональных данных на основе использования правовых мер (название предприятия).

23. Разработка комплексной системы защиты информации на предприятии, осуществляющем изготовление роботов, оснащенных программным обеспечением, представляющем коммерческую тайну (название предприятия).

24. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).

25. Разработка систем видеонаблюдения и сигнализации для обеспечения защиты информации (название предприятия).

26. Организация автоматизированного пропускного режима на крупном предприятии (на примере).

27. Разработка проекта организационных мер по защите аудиоинформации в локальной сети (название предприятия).

28. Разработка комплексной системы защиты информации в кабинете директора (название предприятия).

29. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии.

30. Разработка системы защиты информации конфиденциального характера от утечки по техническим каналам в (название предприятия).

31. Разработка организационного порядка установления внутриобъектного режима для торговой фирмы (название предприятия).

32. Автоматизация обеспечения информационной безопасности группы компаний на базе ОС Unix/Linux.

33. Построение алгоритма системы идентификации, защищенной от подделки продукции.

34. Разработка проекта корпоративной сети (название предприятия).

35. Разработка мероприятий организационного характера по обеспечению комплексной защиты информации для (название предприятия).

36. Разработка систем видеонаблюдения и контроля доступа к объектам информатизации в (название предприятия).

37. Анализ методов и форм работы с персоналом, допущенным к конфиденциальной информации, и разработка рекомендаций по их применению для торговых организаций.

38. Разработка подсистемы защиты от НСД для мобильных устройств предприятия.

39. Разработка подсистемы криптографической защиты информации, передаваемой по каналам связи для мобильных устройств.

40. Защита информации при виртуализации

41. Защита информации на основе использования «облачной» технологии.

Приложение 2

Образец заявления

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Институт компьютерных и инженерных наук
Заведующему кафедрой _____
(полное название кафедры)

_____
(Ф.И.О., ученая степень, ученое звание)

От студента (ки)
_____
(Ф.И.О.)

Группы _____

ЗАЯВЛЕНИЕ

Прошу закрепить за мной выпускную квалификационную работу на тему:
_____
_____
(рабочее полное название темы)

Руководитель:_____
(Ф.И.О., должность, ученая степень, ученое звание)

Дата _____

Подпись студента _____

Руководитель: «Согласен» _____
(подпись)

Дата _____

Решение кафедры:

Зав. кафедрой: _____

Дата: _____

Приложение 3

Пример оформления титульного листа ВКР

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Институт компьютерных и инженерных наук

Кафедра информационной безопасности

Направление подготовки 10.03.01 – Информационной безопасности

Профиль: Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ Л.В. Никифорова
«_____»_____202_ г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка программного обеспечения для тестирования сотрудников ОАО «РЖД» по защите информации

Исполнитель
студент группы 2106–об _____ Е.А. Петров
(подпись, дата)

Руководитель
доцент, канд.техн.наук _____ С.Г. Иванов
(подпись, дата)

Консультанты:
_____ В.В. Скворцов
(подпись, дата)

Нормоконтроль
канд.техн.наук _____ Л.В. Сидоров
(подпись, дата)

Благовещенск 202__

Приложение 4

Образец оформления задания

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Институт_____

Кафедра _____

УТВЕРЖДАЮ
Зав.кафедрой
_____ _____
подпись И.О.Фамилия
«_____»_____ 202_ г,

З А Д А Н И Е

К выпускной квалификационной работе студента _____
_____

1. Тема выпускной квалификационной работы : _____
(утверждена приказом от _____ № _____)

2. Срок сдачи студентом законченной работы (проекта)_____

3. Исходные данные к выпускной квалификационной работе:_____
_____

4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов):
_____
_____

5. Перечень материалов приложения: (наличие чертежей, таблиц, графиков, схем, программных продуктов, иллюстративного материала и т.п.) _____
_____

6. Консультанты по выпускной квалификационной работе (с указанием относящихся к ним разделов)_____
_____

7. Дата выдачи задания_____

Руководитель выпускной квалификационной работы:_____
(фамилия, имя, отчество, должность, ученая степень, ученое звание)

Задание принял к исполнению (дата):_____
(подпись студента)

Приложение 5

Образец оформления реферата

РЕФЕРАТ

Бакалаврская работа содержит 74 с., 26 рисунков, 11таблиц, 4 приложения, 21 источник.

ИНФОРМАЦИОННАЯ БЕЗОНАСНОСТЬ, РАЗРАБОТКА КОМПЛЕКСА ТЕСТОВЫХ ЗАДАНИЙ, КОМПЕТЕНЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ТЕСТИРОВАНИЕ ПЕРСОНАЛА

Цель выпускной квалификационной работы – разработка тестовых заданий для сотрудников ОАО «РЖД» в их компетенциях, определённых предприятием в области защиты информации, на примере отдельного подразделения – ЕИВЦ СП ГВЦ.

В процессе работы был составлен перечень компетенций сотрудников ОАО «РЖД» в области защиты информации.

В результате был разработан комплекс тестовых заданий в рамках компетенций по защите информации.

Приложение 6

Образец оформления нормативных ссылок

В настоящей бакалаврской работе использованы ссылки на следующие стандарты и нормативные документы:

ГОСТ Р 59162 –2020 Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP–сетей

ГОСТ Р 34.10 – 2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 50739–95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ Р 50922–2006 Защита информации. Основные термины и определения

ГОСТ Р 51275–2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 51583–2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

ГОСТ Р 52069.0–2013 Защита информации. Система стандартов. Основные положения

ГОСТ Р 52447–2005 Защита информации. Техника защиты информации. Номенклатура показателей качества

ГОСТ Р 52448–2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения

ГОСТ Р 52633.0–2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации

ГОСТ 19.001–77. Единая система программной документации (ЕСПД). Общие положения.

ГОСТ 19.002–80. ЕСПД. Схемы алгоритмов и программ. Правила выполнения.

ГОСТ 19.004–80. ЕСПД. Термины и определения.

ГОСТ 19.101–77. ЕСПД. Виды программ и программных документов.

ГОСТ 19.102–77. ЕСПД. Стадии разработки.

ГОСТ 19.201–78. ЕСПД. Техническое задание. Требования к содержанию и оформлению.

ГОСТ 19.402–78. ЕСПД. Описание программы.

ГОСТ 19.504–79. ЕСПД. Руководство программиста.

Приложение 7

Пример оформления перечня обозначений и сокращений

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС – автоматизированная система

БД – база данных

ИС – информационная система

ИБ – информационная безопасность

ЛВС − локальная вычислительная сеть

НФ – нормальная форма

ОС – операционная система

ПО – программное обеспечение

РД – руководящий документ

РФ – Российская Федерация

СУБД – система управления базами данных

ФСТЭК – Федеральная служба по техническому и экспортному контролю

Приложение 8

Образец оформления содержания

СОДЕРЖАНИЕ