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

Факультет математики и информатики
Кафедра информационных и управляющих систем

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ КУРСОВОЙ РАБОТЫ

по дисциплине «Организационные меры защиты систем»

для студентов направления подготовки

09.03.02 – «Информационные системы и технологии»

Благовещенск
2017

Методические указания по выполнению курсовой работы по дисциплине «Организационные меры защиты систем» для студентов направления подготовки 09.03.02 Информационные системы и технологии / Составитель С.Г. Самохвалова – Благовещенск.: ФГБОУ ВО «АмГУ», 2017 г. – 30 с.

Методические указания содержат общие и единые требования к содержанию и оформлению текста курсовой работы, а также их защите.

Рецензенты:

Попова Е.Ф доцент, к.т.н., доцент кафедры информатики и методики преподавания информатики ФГБОУ ВО БГПУ

Чалкина Н.А. доцент, к.п.н. доцент кафедры общей математики и информатики ФГБОУ ВО АмГУ

СОДЕРЖАНИЕ

Введение

Убытки от нарушений информационной безопасности могут выражаться в утечке конфиденциальной информации, потере рабочего времени на восстановление данных, ликвидацию последствий вирусных атак и т.п. Убытки могут также выражаться и вполне конкретными суммами, например, когда речь идет о мошенничестве в финансовой сфере с использованием компьютерных систем.

Инвестиции, вложенные организациями в обеспечение ИБ в виде приобретаемых средств защиты информации, оплаты труда специалистов, затрат на проведение внешнего аудита ИБ и т.п., которые неуклонно растут из года в год, зачастую не окупаются. Происходит это потому, что большинство организаций продолжают придерживаться **фрагментарного подхода** к решению проблем информационной безопасности, который оправдывает себя только при условии слабой зависимости организации от информационных технологий и низкого уровня рисков информационной безопасности.

«Фрагментарный» подход направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т. п. Достоинством такого подхода является высокая избирательность к конкретной угрозе. Существенный недостаток — отсутствие единой защищенной среды обработки информации. Фрагментарные меры защиты информации обеспечивают защиту конкретных объектов КС только от конкретной угрозы. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты.

Адекватный уровень информационной безопасности в организации может быть обеспечен только на основе **комплексного подхода**, предполагающего планомерное использование как программно-технических, так и организационных мер защиты на единой концептуальной основе.

Комплексный подход ориентирован на создание защищенной среды обработки информации в КС, объединяющей в единый комплекс разнородные меры противодействия угрозам. Организация защищенной среды обработки информации позволяет гарантировать определенный уровень безопасности КС, что является несомненным достоинством комплексного подхода. К недостаткам этого подхода относятся: ограничения на свободу действий пользователей КС, чувствительность к ошибкам установки и настройки средств защиты, сложность управления.

Организационные меры играют существенно более важную роль и в среднем должны составлять более 60% усилий в этом направлении. Эффективность любых самых сложных и дорогостоящих программно-технических механизмов защиты может быть сведена к нулю в случае игнорирования пользователями ИС элементарных правил парольной политики или нарушения сетевыми администраторами установленных процедур предоставления доступа к ресурсам корпоративной сети. Даже установка дорогостоящих межсетевых экранов не решает проблемы защиты внешнего периметра сети в отсутствии адекватно реализованной политики межсетевых экранов.

Политика безопасности - набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки защищаемой информации, определяя поведение системы в различных ситуациях.

Политика безопасности представляет собой определенный набор требований, прошедших соответствующую проверку, реализуемых при помощи организационных мер и программно-технических средств и определяющих архитектуру системы защиты. Ее реализация для конкретной АС обработки информации осуществляется при помощи средств управления механизмами защиты.

Независимо от предприятия политика безопасности строится на основе нормативно-правовой базы, действующей в государстве, и концептуальных принципах обеспечения безопасности, но при этом конкретная конфигурация программно-аппаратных и технических средств наряду с перечнем инструкций подчеркивает ее индивидуальность.

Для конкретной организации политика безопасности должна быть индивидуальной, зависимой от конкретной технологии обработки информации, используемых программно-аппаратных и технических средств, расположения организации и т.д.

Данные методические рекомендации разработаны с целью выработки единого подхода к подготовке и выполнению курсовой работы, ее оформлению и защите, а также в связи с необходимостью доведения до сведения студентов обязательных требований к содержанию работы, выполнение которых повысит качественный уровень курсовой работы и приведет к экономии затраченного времени.

1. Методические указания по выполнению курсовой работы

1.1 Последовательность выполнения курсовой работы

Для успешного выполнения курсовой работы (далее – КР), необходимо четко определить последовательность ее выполнения: определить совместно с преподавателем тему КР; оформить задание; подобрать литературу, справочники и другие источники по теме исследования; определить структуру КР; обобщить теоретический материал по исследуемой проблеме в соответствии с планом работы; оформить КР; представить работу руководителю; устранить существующие недостатки с учетом рекомендаций руководителя; подготовиться к публичной защите курсовой работы.

1.2 Работа с литературой

Выбрав тему, определите, согласно ей перечень необходимой литературы, периодических изданий и других источников.

Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, ознакомиться с аргументацией их выводов и обобщений, с тем, чтобы на основе анализа, систематизирования, осмысления полученного материала выяснить современное состояние вопроса.

Все свои замечания, выводы по поводу работы с источниками фиксируйте письменно. Записи должны быть краткими, ведите их на отдельных листках.

Записи могут иметь форму плана, тезисов, конспектов, выписок, что в дальнейшем облегчит классификацию и систематизацию полученной информации.

Не забывайте, записи являются лучшим способом накопления и первичной обработки материалов, одной из обязательных форм организации умственного труда.

1.3 Изложение изученного материала

Курсовая работа предполагает обзор литературы по избранной теме, изложение современного состояния вопроса, формулировку выводов и их аргументацию.

Выполнение этих задач облегчается анализом литературы, который проведен студентами при отборе и первичной проработке материала и зафиксирован в конспектах. Теперь особое значение приобретает систематизация сделанных записей и собственных замечаний, предположений и предварительных выводов. Здесь же уточняется и принимается окончательный вариант плана курсовой работы.

В обзоре не следует стремиться к изложению всего и всякого материала, перечисляя одну за другой прочитанные статьи и книги. Необходимо попытаться раскрыть существо вопроса, выделить главные положения и ведущие идеи в соответствии с поставленными задачами и вопросами плана курсовой работы.

Таким образом, обзор должен носить не хронологический, а проблемный характер, раскрывать состояние вопроса по разным литературным источникам. Причем излагать свои мысли следует простым литературным языком, используя общедоступные для понимания термины.

2. Основные разделы курсовой работы

2.1 Структура курсовой работы

Основными элементами структуры КР в порядке их расположения являются следующие:

Титульный лист

Задание

Реферат

Содержание

Введение

Основная часть

Заключение

Библиографический список

Приложения

2.2. Титульный лист

Титульный лист является первой страницей КР, образец титульного листа приведен в приложении 1.

2.3. Задание

Задание на КР выдается в соответствии с требованиями кафедры, форма задания приведена в приложении 2.

2.4. Реферат

Реферат должен содержать: сведения об общем объеме работы, количестве в ней иллюстраций, таблиц, приложений, использованных источников; перечень ключевых слов; текст реферата.

Перечень ключевых слов должен включать от 5 до 15 слов или словосочетаний из текста, которые в наибольшей мере характеризуют его содержание и обеспечивают возможность информационного поиска. Текст реферата должен отражать: объект исследования или разработки; цель работы; метод или методологию выполнения работы; полученные результаты и их новизну; степень внедрения; рекомендации по внедрению; область применения; значимость работы.

Если работа не содержит сведений по какой-либо из перечисленных структурных частей реферата, то в тексте реферата она опускается, при этом последовательность изложения сохраняется.

2.5 Содержание

В содержании приводятся все заголовки КР и указываются страницы, с которых они начинаются. Заголовки содержания должны точно повторять заголовки в тексте. Сокращать или задавать их в другой формулировке, последовательности и соподчиненности по сравнению с заголовками в тексте нельзя.

2.6 Введение

Введение – это вступительная часть работы. Студент должен приложить все усилия, чтобы в этом небольшом по объему разделе показать актуальность темы, но оно не должно быть чересчур пространным и многословным. Основная задача состоит в том, чтобы сделать его убедительным.

Далее следует остановиться на описании степени разработанности темы в научной литературе, сформулировать цели и задачи работы. Требованием к тексту КР является соответствие сформулированной цели и выполнение поставленных задач.

Например,

Целью курсовой работы является разработка политики безопасности для предприятия ПАО «ЮстасБанк».

Для достижения поставленной цели были выделены следующие задачи:

- *анализ предметной области;*
- *анализ и классификация источников угроз информации;*
- *разработка политики информационной безопасности.*

2.7 Основная часть

Основная часть состоит из нескольких глав, каждая из которых имеет свое название. Содержание глав основной части должно точно соответствовать теме КР и полностью ее раскрывать. В конце каждой главы необходимо оформить выводы. Эти главы должны показать умение студента сжато, логично и аргументировано излагать материал.

Основная часть должна соответствовать примерному плану, представленному в данных методических указаниях (п. 4).

2.8 Заключение

В заключении содержатся итоги работы, выводы, к которым пришел автор. Заключение должно быть кратким, обстоятельным и соответствовать поставленным задачам.

Заключительная часть КР подводит итог теоретического и практического поиска студента.

2.9 Библиографический список

Библиографический список являются важнейшим компонентом КР и предназначен для документального подтверждения цитируемого материала, а также для отражения эрудиции автора КР, степени его знакомства с основной литературой в той предметной области, в которой сделана КР. Указываются до 10-15 основных литературных источников, материал которых использован в КР. Особое внимание должно быть уделено изданиям последних лет, так как в них наиболее полно отражен современный подход к решению поставленной проблемы. Все источники нумеруются и на все из них должны быть ссылки в тексте КР.

2.10 Приложения

В приложения рекомендуется «выносить» вспомогательный материал, дополняющий текст КР. Приложения располагаются в конце КР в порядке появления соответствующих ссылок в тексте. Каждое приложение должно иметь заголовок (название), который отражает содержание этого приложения.

3. Требования к курсовой работе

3.1 Требования к изложению текста

Содержание работы должно быть изложено грамотным литературным языком с применением специальной терминологии. В тексте КР необходимо использовать общепринятые в области информационной безопасности понятия и категории. Вопросы темы необходимо исследовать и излагать на основе самостоятельного изучения рекомендованной литературы.

Для научного текста характерна смысловая законченность, целостность и связность. Важнейшим средством выражения логических связей являются специальные функционально-синтаксические средства связи, указывающие на **последовательность развития мысли** (вначале; прежде всего; затем; во-первых; во-вторых; значит; итак и др.), **противоречивые отношения** (однако; между тем; в то время как; тем не менее), **причинно-следственные отношения** (следовательно; поэтому; благодаря этому; кроме того; к тому же), **переход от одной мысли к другой** (прежде чем перейти к.., обратимся к..., рассмотрим, остановимся на..., необходимо рассмотреть), **вывод** (итак; таким образом; значит; в заключение отметим; все сказанное позволяет сделать вывод; подведя итог). В качестве средств связи могут использоваться местоимения, прилагательные и причастия (данные; этот; такой; названные; указанные и др.).

Для образования превосходной степени чаще всего используются слова "наиболее", "наименее". Не употребляется сравнительная степень прилагательного с приставкой "по" (например, "повыше", "побыстрее"), а также превосходная степень прилагательного с суффиксами -айш-, -ейш-, за исключением некоторых терминологических выражений, например, "мельчайшие частицы вещества".

В научной речи очень распространены указательные местоимения "этот", "тот", "такой". Они не только конкретизируют предмет, но и выражают логические связи между частями высказывания (например, "Эти данные служат достаточным основанием для вывода..."). Местоимения "что-то", "кое-что", "что-нибудь" в силу неопределенности их значения в тексте работ обычно не используются.

Обязательным условием объективности изложения материала является также указание на то, каков источник сообщения, кем высказана та или иная мысль, кому конкретно принадлежит то или иное выражение. В тексте это условие можно реализовать, используя специальные вводные слова и словосочетания (по сообщению; по сведениям; по мнению; по данным; по нашему мнению и др.).

Стиль письменной научной речи - это безличный монолог. Поэтому изложение ведется от третьего лица, так как внимание сосредоточено на содержании и логической последовательности сообщения, а не на субъекте. Поэтому нельзя вести изложение от первого лица единственного числа: "я наблюдал", "я считаю", "по моему мнению" и т.п.

Корректнее использовать местоимение "мы", но желательно обойтись без него. Допускаются обороты с сохранением первого лица множественного лица, в которых исключается место-

имение "мы", т.е. фразы строятся с употреблением слов "наблюдаем", "устанавливаем", имеем". Можно использовать выражения: "на наш взгляд", "по нашему мнению", однако предпочтительнее писать "по мнению автора" (курсовой работы) или выражать ту же мысль в безличной форме: "изучение опыта свидетельствует о том, что...", "на основании выполненного анализа можно утверждать...", "проведенные исследования подтвердили..." и т.п.

В тексте работы **не допускается**: применять обороты разговорной речи; применять произвольные словообразования; применять сокращения слов, кроме установленных правилами русской орфографии, соответствующими государственными стандартами.

Напечатанная КР тщательно проверяется. Автор несет полную ответственность за все опечатки как в собственном тексте, так и в цитатах и в научном аппарате.

3.2 Оформление курсовой работы

Текст КР по объему составляет 35-40 страниц машинописного текста (допускается рукописный вариант). Курсовая работа оформляется на стандартных листах бумаги формата А4 и имеет поля: верхнее и нижнее – 20 мм, правое – 10 мм, левое – 30 мм.

Текст курсовой работы оформляется машинописным способом. Межстрочный интервал равен 1,5; размер шрифта – 14 (Times New Roman), цвет шрифта должен быть черным.

В тексте работы необходимо выдерживать абзацы. Абзац состоит из одного или нескольких предложений, имеющих смысловое единство, и выделяется отступом вправо в первой строке на 1,25. Не рекомендуется делать абзацы объёмом более 0,5 страницы.

КР оформляется в соответствии с СТО СМК 4.2.3.05 Стандарт организации. Оформление выпускных квалификационных и курсовых работ (проектов).

3.3 Презентация

Чтобы облегчить восприятие КР, более четко структурировать ее изложение, сделать результаты более наглядными и убедительными, доклад необходимо сопровождать компьютерной презентацией.

Презентации выполняются в среде MS Power Point. При подготовке презентации необходимо заботиться об удобочитаемости материалов с расстояния около трех метров. Презентация (12 – 15 слайдов), оформленная в формате *.ppt или *.pptx, демонстрируется студентом в ходе защиты КР посредством компьютера, LCD - проектора и другими техническими средствами.

3.4 Доклад

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

На защите КР доклад имеет большое значение. Плохой доклад может свести на нет даже отлично выполненную работу.

Основные причины плохого доклада: студент слабо владеет темой КР; отсутствие опыта

публичных выступлений. Это проявляется в неконтролируемых сознанием докладчика, а потому незаметных "для себя" ненужных, а иногда и некрасивых действиях (почесывание, болтание указкой из стороны в сторону, держание руки в кармане, шмыганье носом и т.п.).

Худший вариант, когда доклад читают с листа – "по бумажке".

Хороший доклад на 80 % гарантирует успешную защиту, конечно, при условии, что студент уверенно отвечает на вопросы в ходе защиты. Продолжительность доклада приблизительно 5-7 мин. Основные части доклада, как правило: проблема, решаемая в работе; цель работы; основная часть; заключение (выводы).

4. Основная часть курсовой работы

Примерное содержание курсовой работы.

Введение

1 Анализ предметной области

1.1 Объект защиты. Процессы подлежащие защиты.

1.2 Перечень информации подлежащей защите

2 Основные угрозы ИБ предприятия (объекта защиты)

3 Разработка политики безопасности

3.1 Неформальное описание политики безопасности

3.1.1 Требования безопасности

3.1.2 Нормативные документы и инструкции на предприятии

3.2 Формальное описание политики безопасности

3.2.1 Модель управления доступом

3.2.2 Критерии безопасности

Заключение

Библиографический список

Приложения

4.1. Анализ предметной области

Анализ предметной области является первой фазой разработки политики безопасности (далее – ПБ). Фактически на этом этапе дается ответ на вопрос: «Что и от чего защищать?». Именно здесь лежит ключ к успеху всей работы. Нерешенные вопросы и ошибки, допущенные на этапе анализа, порождают на последующих этапах трудные, часто неразрешимые проблемы и, в конечном счете, приводят к неуспеху всей работы.

Выбор объекта защиты

Сначала необходимо выбрать объект защиты, т.е. нужно решить, что и от чего будем защищать. Объектом защиты может быть и ИС, и отдельно стоящий ПК, а также вся организация в целом. Одним из средств, которые могут помочь в этом, являются поточные диаграммы. С помо-

щью поточных диаграмм необходимо описать взаимосвязи и потоки информации на объекте защиты.

Эффективной методологией для системного анализа предметной области является структурный анализ, включающий поэтапное уточнение функций исследуемого объекта и выявление потоков информации, возникающих между компонентами объекта в результате выполнения поставленной задачи. Для визуализации информационных потоков принято использовать диаграмму потоков данных DFD (Data Flow Diagrams).

Использование методологии структурного анализа

Методы структурного анализа стремятся преодолеть сложность больших систем путем расчленения их на части («черные ящики») и иерархической организации черных ящиков.

Первым шагом упрощения сложной системы является ее разбиение на черные ящики, при этом такое разбиение должно удовлетворять следующим критериям:

каждый черный ящик должен реализовывать единственную функцию системы;

функция каждого черного ящика должна быть легко понимаема независимо от сложности ее реализации;

связь между черными ящиками должна вводиться только при наличии связи между соответствующими функциями системы;

связи между черными ящиками должны быть простыми, насколько это возможно для обеспечения независимости между ними.

Второй важной идеей, лежащей в основе структурных методов, является идея иерархии. Для понимания сложной системы недостаточно разбиения ее на части, необходимо эти части организовать определенным образом, а именно в виде иерархических структур.

Третий момент: структурные методы широко используют графические нотации, также служащие для облегчения понимания сложных систем.

Структурным анализом принято называть метод исследования системы, который начинается с ее общего обзора и затем детализируется, приобретая иерархическую структуру с большим числом уровней.

Все методологии структурного анализа базируются на ряде общих принципов. В качестве двух базовых принципов используются следующие: **принцип «разделяй и властвуй» и принцип иерархического упорядочивания.**

Первый является принципом решения трудных, проблем путем разбиения их на множество меньших независимых задач, легких для понимания и решения.

Второй принцип в дополнение к тому, что легче понимать проблему, если она разбита на части, декларирует, что устройство этих частей существенно для понимания.

Понимание проблемы резко повышается при организации ее частей в древовидные иерархические структуры, т.е. система может быть понята и построена по уровням, каждый из которых добавляет новые детали.

Выделение двух базовых принципов не означает, что остальные принципы являются второстепенными, игнорирование любого из них может привести к непредсказуемым последствиям. Основные принципы:

принцип абстрагирования заключается в выделении существенных аспектов системы и отвлечении от несущественных с целью представления проблемы в простом общем виде;

принцип формализации заключается в необходимости строгого методического подхода к решению проблемы;

принцип упрятывания заключается в упрятывании несущественной на конкретном этапе информации: каждая часть «знает» только необходимую ей информацию;

принцип полноты заключается в контроле на присутствие лишних элементов;

принцип непротиворечивости заключается в обоснованности и согласованности элементов;

принцип логической независимости заключается в концентрации внимания на логическом проектировании для обеспечения независимости от физического проектирования;

принцип независимости данных заключается в том, что модели данных должны быть проанализированы и спроектированы независимо от процессов их логической обработки, а также от их физической структуры и распределения;

принцип структурирования данных заключается в том, что данные должны быть структурированы и иерархически организованы.

Руководство всеми принципами в комплексе позволяет на более ранних стадиях разработки понять, что будет представлять собой создаваемая система, обнаружить промахи и недоработки.

Для целей моделирования систем вообще, и структурного анализа в частности, используются три группы средств, иллюстрирующих:

функции, которые система должна выполнять;

отношения между данными;

зависящее от времени поведение системы (аспекты реального времени).

Среди всего многообразия средств решения данных задач в методологиях структурного анализа наиболее часто и эффективно применяемыми являются следующие:

- **DFD** (Data Flow Diagrams) - диаграммы потоков данных совместно со словарями данных и спецификациями процессов;
- **ERD** (Entity-Relationship Diagrams) - диаграммы «сущность-связь»;
- **STD** (State Transition Diagrams) - диаграммы переходов состояний.

Все они содержат графические и текстовые средства моделирования: первые - для удобства демонстрирования основных компонентов модели, вторые - для обеспечения точного определения ее компонентов и связей.

Перечисленные средства дают полное описание системы независимо от того, является ли она существующей или разрабатывается с нуля.

Диаграммы потоков данных являются основным средством моделирования функциональных требований проектируемой системы. С их помощью эти требования разбиваются на функциональные компоненты и представляются в виде сети, связанной потоками данных. Главная цель. таких средств - продемонстрировать, как каждый процесс преобразует свои входные данные в выходные, а также выявить отношения между этими процессами.

Главная цель построения иерархического множества DFD заключается в том, чтобы сделать требования ясными и понятными на каждом уровне детализации, а также разбить эти требования на части с точно определенными отношениями между ними. **Для достижения этого целесообразно пользоваться следующими правилами**:

- Размещать на каждой диаграмме от 3 до 7 процессов. Верхняя граница соответствует человеческим возможностям одновременного восприятия и понимания структуры сложной системы с множеством внутренних связей, нижняя граница выбрана по соображениям здравого смысла: нет необходимости детализировать процесс диаграммой, содержащей всего один или два процесса.
- Не загромождать диаграммы несущественными на данном уровне деталями.
- Декомпозицию потоков данных осуществлять параллельно с декомпозицией процессов; эти две работы должны выполняться одновременно, а не одна после завершения другой.
- Выбирать ясные, отражающие суть дела, имена процессов и потоков для улучшения понимания диаграмм,
- Однократно определять функционально идентичные процессы на самом верхнем уровне, где такой процесс необходим, и ссылаться к нему на нижних уровнях.
- Пользоваться простейшими диаграммными техниками: если что- либо возможно описать с помощью DFD, то это и необходимо делать, а не использовать для описания более сложные объекты.
- Отделять управляющие структуры от обрабатывающих структур (т.е. процессов), локализовать управляющие структуры.

В соответствии с этими рекомендациями процесс построения модели разбивается на следующие этапы:

- Расчленение множества требований и организация их в основные функциональные группы.
- Идентификация внешних объектов, с которыми система должна быть связана.
- Идентификация основных видов информации, циркулирующей между системой и внешними объектами.
- Предварительная разработка контекстной диаграммы, на которой основные функциональные группы представляются процессами, внешние объекты - внешними сущностями, основные виды информации - потоками данных между процессами и внешними сущностями.

- Изучение предварительной контекстной диаграммы и внесение в нее изменений по результатам ответов на возникающие при изучении вопросов по всем ее частям.
- Построение контекстной диаграммы путем объединения всех процессов предварительной диаграммы в один процесс, а также группирования потоков.
- Формирование DFD первого уровня на базе процессов предварительной контекстной диаграммы.
- Проверка основных требований по DFD первого уровня.
- Декомпозиция каждого процесса текущей DFD с помощью детализирующей диаграммы или спецификации процесса.
- Проверка основных требований по DFD соответствующего уровня.
- Добавление определенных новых потоков в словарь данных при каждом их появлении на диаграммах.
- Параллельное (с процессом декомпозиции) изучение требований, разбиение их на элементарные и идентификация процессов или спецификации процессов, соответствующих этим требованиям.
- После построения двух-трех уровней проведение ревизии с целью проверки корректности и улучшения понимания модели.
- Построение спецификации процесса (а не простейшей диаграммы) в случае, если некоторую функцию сложно или невозможно выразить комбинацией процессов.

4.2. Перечень информации, подлежащей защите

На данном этапе студент должен привести перечень информации, подлежащей защите, основываясь на нормативных документах РФ, а также на внутренних документах организации. Защите подлежат как сведения, составляющие государственную тайну, так и конфиденциальные сведения.

По своему содержанию конфиденциальная информация включает все виды существующих тайн, определенных Законодательством РФ, за исключением государственной тайны.

К конфиденциальной информации относится и коммерческая тайна. В настоящее время информация, составляющая коммерческую тайну, является наиболее распространенной, поскольку охватывает все сферы деятельности коммерческих и государственных предприятий, накапливается и хранится в налоговых органах, органах Минюста, других органах государственной власти, в учреждениях науки и культуры. Согласно закону №24-ФЗ, конфиденциальная информация - информация ограниченного доступа, и она защищается законодательством.

Отнесение сведений к конфиденциальной информации

Отнесение сведений к конфиденциальной информации осуществляется в порядке, установленном законодательством РФ и в соответствии с "Перечнем сведений конфиденциального характера", утвержденным Указом Президента РФ от 6.03.97г. №188. К сведениям **конфиденциального характера данный перечень относит:**

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским Кодексом РФ и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью; доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Необходимость установления ограничений доступа к различным видам тайн, определенным в законодательстве РФ, не является самоцелью. Это реализация прав и свобод граждан, организаций, учреждений, определенных Конституцией РФ (ст.ст. 23, 24.1). Вместе с тем Конституция гарантирует права на доступ к определенной информации (ст.24.2, 29.4,5; 42) и ответственность должностных лиц за ее сокрытие.

Запрещено относить к информации с ограниченным доступом, и в том числе к конфиденциальной, следующие документы:

законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением отнесенных к государственной тайне;

документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Следует выделить три условия, выполнение которых позволяет рассматривать информацию как служебную или коммерческую тайну и относить ее к конфиденциальной.

Во-первых, информация должна иметь действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. Это означает, что знание и использование ее третьими лицами может нанести материальный или иной ущерб органу государственной власти, предприятию, организации, учреждению, как с государственной, так и с не государственной формой собственности.

Во-вторых, к ней нет свободного доступа на законном основании. Это означает, что данная информация не относится к информации, которую законом запрещено относить к конфиденциальной.

В-третьих, обладатель информации принимает меры к охране ее конфиденциальности. Это означает, что обладатель обязан применять меры по ограничению доступа всеми законными способами, предусмотренными законодательством РФ. К таким мерам следует отнести: организационные и нормативно-правовые, ограничивающие доступ к носителям информации; использование только сертифицированных средств защиты (программных и технических) и другие.

Примерный перечень сведений, составляющих коммерческую тайну.

ПРОИЗВОДСТВО: Сведения о структуре и масштабах производства, производственных мощностях, типе и размещении оборудования, запасах сырья, материалов и готовой продукции.

УПРАВЛЕНИЕ: Сведения о применяемых оригинальных методах управления организацией. Сведения о подготовке, принятии и исполнении отдельных решений руководства организации по коммерческим, организационным, научно-техническим и иным вопросам.

ПЛАНЫ: Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях. Также сведения инвестиций, закупок и продаж.

СОВЕЩАНИЯ: Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления организации.

ФИНАНСЫ: Сведения о кругообороте средств организации, финансовых операциях, состоянии банковских счетов организации и проводимых операциях, об уровне доходов организации, о состоянии кредита организации (пассивы и активы).

РЫНОК: Сведения о применяемых организацией оригинальных методах изучения рынка (маркетинга). Сведения о результатах изучения рынка, содержащие оценки состояния и перспектив развития рыночной конъюнктуры. Сведения о рыночной стратегии организации, о применяемых организацией оригинальных методах осуществления продаж, об эффективности служебной и коммерческой деятельности организации

ПАРТНЕРЫ: Обобщенные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах, состоящих в деловых отношениях с организацией.

КОНКУРЕНТЫ: Обобщенные сведения о внутренних и зарубежных предприятиях как о потенциальных конкурентах в деятельности организации, оценка качества деловых отношений с конкурирующими предприятиями в различных сферах деловой активности.

ПЕРЕГОВОРЫ: Сведения о подготовке, проведении и результатах переговоров с деловыми партнерами организации.

КОНТРАКТЫ: Сведения об условиях конфиденциальности, из которых можно установить порядок соглашения и другие обязательства организации с партнерами (клиентами).

ЦЕНЫ: Сведения о методах расчета, структуре, уровнях реальных цен на продукцию и размеры скидок.

ТОРГИ, АУКЦИОНЫ: Сведения о подготовке к участию в торгах и аукционах, результатах приобретения или продажи на них товаров.

НАУКА И ТЕХНИКА: Сведения о целях, задачах, программах перспективных научных исследований. Ключевые идеи научных разработок, точные значения конструкционных характеристик, создаваемых изделий и оптимальных параметров разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т.д.). Аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи, данные об условии экспериментов и оборудовании, на котором они проводились. Сведения о материалах, из которых изготовлены отдельные детали, об особенностях конструкторско-технологического, художественно-технического решения изделия, дающие положительный экономический эффект. Сведения о методах защиты от подделки товарных и фирменных знаков, о состоянии парка ПЭВМ и программного обеспечения.

ТЕХНОЛОГИЯ: Сведения об особенностях используемых и разрабатываемых технологий и специфике их применения, об условиях их производства и транспортировке продукции.

БЕЗОПАСНОСТЬ: Сведения о порядке и организации защиты коммерческой тайны, о порядке и состоянии организации охраны, системы сигнализации, пропускном режиме.

4.3. Угрозы

В данном разделе курсовой работы студент определяет угрозы, которым подвержена защищаемая информация, вращающаяся в организации. Все угрозы можно поделить на внутренние и внешние.

Существует три основных типа угроз: угрозы, обусловленные действиями субъекта (антропогенные); угрозы, обусловленные техническими средствами (техногенные); угрозы, обусловленные стихийными источниками.

Антропогенными источниками угроз безопасности выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Эта группа наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от воли организаторов защиты.

Вторая группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако последствия, вызванные такой деятельностью, вышли из-под контроля человека и существуют сами по себе. Человечество становиться всё более зависимым от техники, и источники угроз, которые напрямую зависят от свойств техники менее прогнозируемые, и поэтому требуют особого внимания.

Третья группа источников угроз объединяет обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить, или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию, и поэтому меры защиты от них должны применяться всегда. Стихийные источники потенциальных угроз ИБ, как правило, являются внешними к защищаемому объекту и под ними понимаются, прежде всего, природные катаклизмы. Таблица содержит примерный перечень источников угроз безопасности для организации, работающей с информацией, содержащей коммерческую тайну.

Источники угроз безопасности
Антропогенные источники
Внешние антропогенные источники
Криминальные структуры
Недобросовестные партнёры
Представители надзорных организаций и аварийных служб
Внутренние антропогенные источники[1]
Основной персонал
Представители службы безопасности
Вспомогательный персонал (уборщики, охрана)
Технический персонал (жизнеобеспечение, эксплуатация)
Техногенные источники
Внешние техногенные источники
Транспорт
Внутренние техногенные источники
Некачественные технические средства
Стихийные источники
Внешние стихийные источники
Пожары
Землетрясение
Наводнения
Ураганы
Радиоактивное излучение
Различные непредвиденные обстоятельства
Другие форс-мажорные обстоятельства

Примечания:

Особую группу внутренних антропогенных источников составляют специально внедрённые и завербованные агенты из числа основного, вспомогательного, технического персонала и представителей службы безопасности. Эта группа не рассматривается как самостоятельная, но при анализе, в случае возникновения потенциальной возможности внедрения агентов, необходимо учитывать особенности защиты от таких источников при рассмотрении возможностей внутренних антропогенных источников.

В данном случае под термином "другие форс-мажорные обстоятельства" понимается юридическая составляющая форс-мажора, то есть различные решения высших государственных органов, забастовки, войны, революции и т.п., приводящие к возникновению обстоятельств непреодолимой силы.

Для выбора средств защиты информации в ходе анализа угроз полезно определить условия реализации и их источники.

Все угрозы являются потенциальными, а значит, могут остаться и нереализованными. Для реализации угроз необходимы некоторые условия:

в наличие каналов утечки; при этом, под каналом утечки понимается совокупность источника сообщения, среды его распространения и нелегитимного приемника - преобразователя сообщений; наличие каналов информационного воздействия; при этом под каналом информационного воздействия понимается совокупность источника воздействия, среды его передачи и объекта воздействия (носителя информации);

отсутствие прогнозирования поведения системы при поступлении в нее новой информации, в результате чего может иметь место неадекватная реакция службы безопасности на возможные действия нарушителя.

Из всего сказанного можно сделать вывод: система может находиться в безопасном состоянии только при принятии мер направленных на устранение условий реализации угроз.

4.4. Разработка политики безопасности

Неформальное описание политики безопасности

Политика безопасности - это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

Политика безопасности - это совокупность программных, аппаратных, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, четко регламентирующих все аспекты деятельности организации или предприятия, включая информационную систему и систему, обеспечивающую безопасность предприятия и организации .

Требования безопасности

В данном пункте работы студент должен предъявить те требования безопасности, которые он выдвигает к защищаемой информации. К примеру, часть информации может быть предоставлена любому сотруднику данной организации, но не должна выходить за пределы организации, а

другая информация предоставляется ограниченному числу сотрудников организации по письменному запросу. Т.е. к информации разного уровня доступа предъявляются разные требования безопасности.

Требования к интерфейсу взаимодействия с ИС:

формирование разграничения доступа.

соблюдение законодательства РФ.

устав предприятия.

наличие плана действий при возникновении непредвиденной ситуации.

После построения интерфейса взаимодействия с ИС обязательной составляющей ПБ является определение ответственности в случае нарушения данной политики.

Наличие плана действий организации или предприятия в случае непредвиденной ситуации. Данное требование необходимо для поддержания непрерывной работоспособности комплексной системы защиты информации.

Разработка и совершенствование ПБ представляет собой непрерывный процесс, обусловленный следующими факторами:

- изменение ценности информации;
- изменение архитектуры ИС;
- изменение применяемых ИТ;
- изменение совокупности угроз;
- изменение технологии НСД (несанкционированного доступа).

Политика безопасности - совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определения множества угроз и составляет необходимое, а иногда и достаточное условие безопасности системы; формальное выражение ПБ называют моделью ПБ, основная цель которой формальное доказательство критерия безопасности. Критерий безопасности описывает те условия, при выполнении которых модель будет безопасной при переходе из одного состояния в другое.

Пример. Пример посвящен проблеме компромисса задачи защиты и других задач вычислительной системы. Пусть в базе данных собирается информация о здоровье частных лиц, которая в большинстве стран считается конфиденциальной. База данных нужна, т.к. эта информация позволяет эффективно производить диагностику. Если доступ к этой базе из соображений защиты информации сильно ограничен, то в такой базе не будет пользы для врачей, ставящих диагнозы, и не будет пользы от самой базы. Если доступ открыть, то возможна утечка конфиденциальной информации, за которую по суду может быть предъявлен большой иск. Каким должно быть оптимальное решение?

Результатом решения в данном примере и других аналогичных задачах является выбор правил распределения и хранения информации, а также обращения с информацией, что и называется политикой безопасности.

Соблюдение ПБ должно обеспечить выполнение того компромисса между альтернативами, который выбрали владельцы ценной информации для ее защиты. Являясь результатом компромисса, ПБ никогда не удовлетворит все стороны, участвующие во взаимодействии с защищаемой информацией.

В тоже время выбор ПБ - это окончательное решение проблемы: что - хорошо и что - плохо в обращении с ценной информацией. После принятия такого решения можно строить защиту, то есть систему поддержки выполнения правил ПБ. Таким образом, построенная система защиты информации хорошая, если она надежно поддерживает выполнение правил ПБ. Наоборот, система защиты информации - плохая, если она ненадежно поддерживает ПБ.

Нормативные документы и инструкции на предприятии

На данном этапе работы студенту необходимо привести список нормативных документов предприятия, в которых определяются: защищаемая информация, средства и методы защиты, ответственные за защиту лица и другие документы, регламентирующие защиту информации на предприятии.

В данный список могут быть включены: устав предприятия, т.к. в нем говорится, что в организации есть защищаемая информация и что эта организация будет осуществлять меры по ее защите; положение о структурном подразделении по защите информации; перечень защищаемой информации; перечень допущенных лиц; должностная инструкция специалиста по защите информации; инструкции по парольной защите, по антивирусной защите, о резервном копировании и т.д.

Формальное описание политики безопасности

Модели управления доступом играют основную роль в методе формальной разработки ПБ. Данная модель определяет правила управления доступом к информации, контролирует потоки информации между субъектами и объектами доступа на предмет удовлетворения критерию безопасности системы защиты информации. Целью этой модели является выражение сути требований по безопасности к данной системе.

Принципы создания ПБ.

1. Принцип системности.
2. Принцип комплексности.
3. Принцип непрерывности защиты.
4. Принцип разумной достаточности.
5. Принцип открытости алгоритмов и механизмов защиты.
6. Принцип простоты применения средств защиты.
7. Принцип использования нескольких специализированных нормативных документов.

Обоснование выбора модели управления доступом

Первым и основным обоснованием является форма собственности предприятия, она подвержена влиянию законодательству - либо требует (государственные организации), либо опреде-

ляется собственником (коммерческие организации). Из этого вытекают требования к системе безопасности, и далее рассматривается экономический аспект. При наличии в организации сведений, содержащих государственную тайну, первичным обоснованием является выполнение требований законодательства.

В результате студент должен, проанализировав все особенности выбранной им организации, выбрать модель управления доступом и привести обоснования, почему именно эта модель была выбрана.

На сегодняшний день используются четыре основных класса моделей управления доступом:

1. Дискреционные модели управления доступом – модели, в которых владелец ресурса сам задает права доступа к нему. В большинстве случаев права доступа субъектов к объектам представляются в виде матрицы или списков доступа.

2. Мандатные модели управления доступом, в которых режим доступа субъектов к объектам определяется установленным режимом конфиденциальности.

3. Ролевая модель управления доступом, копирующая иерархическую структуру организации и позволяющая упростить администрирование.

4. Атрибутная модель, являющаяся наиболее универсальной и позволяющая контролировать доступ с учетом произвольных параметров среды, субъектов и объектов доступа.

Дискреционная модель управления доступом

Классической дискреционной моделью управления доступом является модель Харрисона-Руззо-Ульмана, которая реализует произвольное управление доступом субъектов к объектам и контроль распределения прав доступа.

В рамках этой модели система обработки информации представляется в виде совокупности активных сущностей - субъектов, которые осуществляют доступ к информации, пассивных сущностей - объектов, содержащих защищаемую информацию, и конечного множества прав доступа, означающих полномочия на выполнение соответствующих действий (например, чтение, запись, выполнение).

Модель безопасности Харрисона-Руззо-Ульмана формализует понятие матрицы доступа – таблицы, описывающей права доступа субъектов к объектам.

Строки матрицы доступа соответствуют субъектам, существующим в системе, а столбцы – объектам. На пересечении строки и столбца указаны права доступа соответствующего субъекта к данному объекту.

Классическая модель Харриона-Руззо-Ульмана до сих пор широко используется при проведении формальной верификации корректности построения систем разграничения доступа в высоко защищенных автоматизированных системах. Развитие моделей дискреционного управления доступом заключается преимущественно в построении всевозможных модификаций модели Харрисона-Руззо-Ульмана, а также в поиске минимально возможных ограничений, которые

можно наложить на описание системы, чтобы вопрос ее безопасности был вычислительно разрешимым.

Мандатная модель управления доступом

Одной из самых известных моделей мандатного управления доступа является модель Белла-ЛаПадулы.

Мандатный принцип разграничения доступа, изначально, ставил своей целью перенести на автоматизированные системы практику секретного документооборота, принятую в правительственных и военных структурах, когда все документы и допущенные к ним лица ассоциируются с иерархическими уровнями секретности.

Основным положением политики Белла-ЛаПадулы, взятым ими из реальной жизни, является назначение всем участникам процесса обработки защищаемой информации, и документам, в которых она содержится, специальной метки, например, секретно, совершенно секретно и т.д., получившей название метки безопасности. Все уровни безопасности упорядочиваются с помощью установленного отношения доминирования, например, уровень совершенно секретно считается более высоким чем уровень секретно, или доминирует над ним. Контроль доступа осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании двух простых правил:

1. Уполномоченное лицо (субъект) имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности.

2. Уполномоченное лицо (субъект) имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности.

Первое правило обеспечивает защиту информации, обрабатываемой более доверенными (высокоуровневыми) лицами, от доступа со стороны менее доверенных (низкоуровневых). Второе правило предотвращает утечку информации (сознательную или несознательную) со стороны высокоуровневых участников процесса обработки информации к низкоуровневым.

Критерии безопасности формулируются следующим образом:

• состояние системы является безопасным по чтению тогда и только тогда, когда для каждого индивидуального или группового субъекта, имеющего в этом состоянии доступ чтения к объекту, наибольшая нижняя граница множества уровней безопасности этого субъекта доминирует над уровнем безопасности этого объекта.

• состояние системы является безопасным по записи; тогда и только тогда, когда для каждого индивидуального или группового субъекта, имеющего в этом состоянии доступ записи к объекту, уровень безопасности этого объекта доминирует над наименьшей верхней границей множества уровней безопасности этого субъекта.

Система безопасна тогда и только тогда, когда ее начальное состояние безопасно и все состояния, достижимые из начального, путем применения конечной последовательности запросов из множества запросов, безопасны.

Ролевая модель управления доступом

Ролевая модель управления доступом содержит ряд особенностей, которые не позволяют отнести ее ни к категории дискреционных, ни к категории мандатных моделей.

Основная идея реализуемого в данной модели подхода состоит в том, что понятие «субъект» заменяется двумя новыми понятиями:

пользователь – человек, работающий в системе;

роль – активно действующая в системе абстрактная сущность, с которой связан ограниченный и логически непротиворечивый набор полномочий, необходимых для осуществления тех или иных действий в системе.

С точки зрения ролевой политики имеет значение не личность пользователя, осуществляющего доступ к информации, а то какие полномочия ему необходимы для выполнения его служебных обязанностей. Кроме того, количество ролей в системе может не соответствовать количеству реальных пользователей: один пользователь, если на нем лежат различные обязанности, требующие различных полномочий, может выполнять (одновременно или последовательно) несколько ролей; а несколько пользователей могут пользоваться одной и той же ролью, если они выполняют одну и туже работу. Полномочия назначаются ролям в соответствии с принципом наименьших привилегий, из которого следует, что каждый пользователь должен обладать только минимальным, необходимым для выполнения своей работы, набором полномочий.

Основным достоинством ролевой модели является близость к реальной жизни: роли, действующие в ИС, могут быть выстроены в полном соответствии с корпоративной иерархией и при этом привязаны не к конкретным пользователям, а к должностям – что, в частности, упрощает администрирование в условиях большой текучки кадров.

Атрибутная модель управления доступом

Атрибутная модель управления доступом является наиболее универсальной. Основная идея данной модели заключается в том, что решение о предоставлении доступа субъекта к объекту принимается на основе анализа набора произвольных атрибутов, связанных с субъектом, объектом или даже средой их функционирования. Каждый атрибут представляет собой некий набор данных, который может быть сопоставлен с массивом допустимых значений данного атрибута.

Для получения доступа к объекту субъект предъявляет некий имеющийся у него набор атрибутов. Монитор безопасности обращений сравнивает значение каждого атрибута с перечнем допустимых, и в случае, если все атрибуты являются допустимыми, предоставляет доступ.

Можно выделить два основных подхода к использованию формальных моделей управления доступом непосредственно при проведении оценки соответствия средств защиты информации:

1. Независимый контроль факта реализации той или иной модели в системе, а также контроль выполнения формального критерия безопасности (если применимо).

2. Формальное доказательство тех или иных положений с использованием инструментария той или иной модели.

Первый подход, в частности, характерен для ролевой модели или модели Белла-ЛаПадулы, а второй – для модели Харрисона-Руззо-Ульмана.

Критерий безопасности

Критерий безопасности является необходимой частью модели управления доступом, так как он описывает те условия, при выполнении которых модель будет безопасной при переходе из одного состоянии в другое, т.е. не будет несанкционированного доступа или утечки. Для каждой модели существует свой критерий безопасности, но при этом все они схожи в одном: система должна иметь начальное безопасное состояние. На данном этапе студент должен доказать, что разработанная им система удовлетворяет критерию безопасности выбранной им модели управления доступом, написать критерий безопасности и начальные условия.

При выполнении данной курсовой работой студент должен освоить:

1. Методологию структурного анализа предметной области.
2. Нормативные документы, регламентирующие отнесение сведений к конфиденциальной информации.
3. Существующие угрозы безопасности и научиться выбирать те, которые присущи конкретной информационной системе.
4. Научится выбирать и применять модели управления доступом при создании политики безопасности организации.

В результате работы студент должен разработать ПБ объекта, при этом необходимо обосновать, что выбранная ПБ адекватна требованиям информационной безопасности.

5. Порядок защиты и критерии оценки

5.1. Порядок защиты курсовой работы

КР представляется и защищается в сроки, предусмотренные графиком выполнения КР по дисциплине «Организационные меры защиты систем»**.** Студент обязан представить на проверку научному руководителю окончательный вариант курсовой работы не менее чем за 5 дней до назначенной даты защиты курсовых работ. Если КР не представлена в назначенный срок по уважительной причине, студенту определяется новый срок представления работы. Если КР была представлена в срок, но при этом не соответствовала требованиям по содержанию и/или оформлению, то такая работа возвращается студенту для доработки.

КР допускается к защите при условии соответствия ее содержания и оформления требованиям, сформулированным в данных методических указаниях и соблюдения сроков предоставления. Защита КР происходит перед комиссией в количестве 2-3 преподавателей, один из которых руководитель КР.

Процедура защиты состоит из краткого выступления студента, в котором должны быть отражены основные направления исследования и сформулированы его результаты, ответов сту-

дента на вопросы. Задачей студента при защите является не пересказ того, как написано в литературе, а что сделано им самим при изучении проблемы.

5.2. Критерии оценки курсовой работы

Критериями оценки курсовой работы являются:

качество содержания работы (полнота раскрытия темы, отражение знаний литературы и различных точек зрения по теме, аргументированное обоснование выводов и предложений);

логика, грамотность и научный стиль изложения;

соблюдение графика выполнения курсовой работы;

внешний вид работы и ее оформление, аккуратность;

соблюдение заданного объема работы;

качество оформления рисунков, схем, таблиц;

правильность оформления библиографического списка;

достаточность и новизна изученной литературы;

содержательность выступления;

наличие качественной презентации;

правильные ответы на вопросы при защите.

Оценивается работа по 4-х балльной системе (отлично, хорошо, удовлетворительно, неудовлетворительно).

Оценка **«отлично»** выставляется при выполнении КР в полном объеме; работа отличается глубиной проработки всех разделов содержательной части, оформлена с соблюдением установленных правил; студент свободно владеет теоретическим материалом,; на все вопросы дает правильные и обоснованные ответы, убедительно защищает свою точку зрения.

Оценка **«хорошо»** выставляется при выполнении КР в полном объеме; работа отличается глубиной проработки всех разделов содержательной части, оформлена с соблюдением установленных правил; студент твердо владеет теоретическим материалом, может применять его самостоятельно; на большинство вопросов даны правильные ответы, защищает свою точку зрения достаточно обоснованно.

Оценка **«удовлетворительно»** выставляется при выполнении КР в основном правильно, но без достаточно глубокой проработки некоторых разделов; студент усвоил только основные разделы теоретического материала; на вопросы отвечает неуверенно или допускает ошибки, неуверенно защищает свою точку зрения.

Оценка **«неудовлетворительно»** выставляется, когда студент не может защитить свои решения, допускает грубые ошибки при ответах на поставленные вопросы или не отвечает на них.

Положительная оценка выставляется в ведомость и зачетную книжку. Студент, получивший неудовлетворительную оценку, должен доработать КР.

Список использованных источников

1. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. М: ДНК, 2012

2. Баранова, Е. К. Информационная безопасность и защита информации / Е. К. Баранова, А. В. Бараш. − М.: ЕАОИ, 2012. − 312 с.

3. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности / Н.С. Кармановский, О.В. Михайличенко, С.В. Савков. – СПб.: НИУ ИТМО, 2013. – 148 с.

4. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. – 5-е изд., стер. – М.: Академия, 2011. – 330 с.

5. Ярочкин, В.И. Информационная безопасность: Учебник / В. И. Ярочкин. - МО. - М. : Академический Проект, 2008.

6. Марков, А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / А.С.Марков, В.Л.Цирлов, А.В.Барабанов; под ред. А.С.Маркова. - М.: Радио и связь, 2012. 192 с.

7. Суркова, Н.Е. Методология структурного проектирования информационных систем: Монография / Н.Е. Суркова, А.В. Остроух. Красноярск: Научно-инновационный центр, 2014. 190 с.

8. Моделирование управляемых процессов: конспект лекций / А.А. Ступина, С.Н. Еженаманская, Л.Н. Корпачёва, А.В. Фёдорова; ФГОУ ВПО СибФУ. – Красноярск, 2008. – 158 с.

9. Методические указания по выполнению курсовых по дисциплине «Организационное и правовое обеспечение информационной безопасности» для студентов направления подготовки «Информационная безопасность»/ Составитель Н.Ш.Козлова - Майкоп: Изд-во МГТУ, 2013. -16 с.

10. Паршуков, Д. В. Информационная безопасность: метод. указания по выполнению курсовой работы / Д. В. Паршуков; Красноярский государственный аграрный ун-т, Ачинский ф-л. – Красноярск, 2016. – 20 с.

11. Паршин, К.А., Червинский, А.Н. Разработка политики безопасности на объекте: методические указания к курсовой работе по дисциплине «Теория информационной безопасности и методология защиты информации» для студентов 3 курса специальности «Организация и технология защиты информации»/ К. А. Паршин, А.Н. Червинский; уральский государственный университет путей сообщения. – Екатеринбург, 2005. – 35 с.

12. Аверченков, В.И. Системы организационного управления [Электронный ресурс]: учебное пособие/ Аверченков В.И., Ерохин В.В.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 208 c.— Режим доступа: http://www.iprbookshop.ru/7013.— ЭБС «IPRbooks»

13. Учебно-методическое пособие по выполнению курсового проекта по дисциплине «Методы и средства защиты информации в компьютерных сетях» [Электронный ресурс]/ — Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2015.— 35 c.— Режим доступа: http://www.iprbookshop.ru/61741.— ЭБС «IPRbooks»

14. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 c.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks»

15. Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 c.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks»

16. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2010.— 544 c.— Режим доступа: http://www.iprbookshop.ru/7943.— ЭБС «IPRbooks»

17. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 c.— Режим доступа: http://www.iprbookshop.ru/52209.— ЭБС «IPRbooks», по паролю

Приложение 1

Образец титульного листа курсовой работы

Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.03.02 – Информационные системы и технологии

КУРСОВАЯ РАБОТА

на тему: Разработка политики безопасности для ООО «Техпомощь»

по дисциплине «Организационные меры защиты систем »

Исполнитель
студент группы 354 _____ В.В. Сидоров
(подпись, дата)

Руководитель
доцент, канд.техн.наук _____ А.В. Иванов
(подпись, дата)

Нормоконтроль
доцент, канд.техн.наук _____ И.П. Петрошевский
(подпись, дата)

Благовещенск 2017

Приложение 2

Форма задания на выполнение курсовой работы

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

Факультет_____
Кафедра _____

З А Д А Н И Е

К курсовой работе студента _____
_____

1. Тема курсовой работы:_____
_____
2. Срок сдачи студентом законченной работы _____

3. Исходные данные к курсовой работе:_____
_____
_____

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

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

Руководитель курсовой работы _____
(фамилия, имя, отчество, должность, ученая степень, ученое звание)

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