С А Н К Т - П Е Т Е Р Б У Р Г С К И Й У Н И В Е Р С И Т Е Т
У П Р А В Л Е Н И Я И Э К О Н О М И К И

АЛТАЙСКИЙ ИНСТИТУТ ЭКОНОМИКИ

ЭКОНОМИКО-ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра ЭКОНОМИКИ И МЕНЕДЖМЕНТА

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ КОНТРОЛЬНЫХ РАБОТ

дисциплины Основы информационной безопасности

для направлений подготовки бакалавров

080200.62 «Менеджмент»

030900.62 «Юриспруденция»

Барнаул

2014

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

_ Грибова Г.В., к.п.н., доцент /_____/
(инициалы и фамилия, ученая степень и ученое звание) (подпись)

Методические рекомендации обсуждены на заседании кафедры

Экономики и менеджмента_____ «____»_____20___г.,

протокол №__.

Заведующий кафедрой _С.Ю. Шевелев_/_____/
(инициалы и фамилия) (подпись)

Содержание

Общие положения

Написание контрольной работы по дисциплине «Основы информационной безопасности» является необходимым элементом учебного процесса при подготовке бакалавров менеджмента/юриспруденции.

Основной целью выполнения контрольной работы является развитие мышления, творческих способностей студента, привитие ему навыков самостоятельной работы, связанной с поиском, систематизацией и обобщением существующих нормативно-правовых документов, а также имеющейся научной и учебной литературы, формирование умений анализировать и критически оценивать исследуемый научный и практический материал, а также продемонстрировать отдельные практические навыки обработки информации средствами ПЭВМ.

Тема контрольной работы определяется студентом по согласованию с преподавателем в пределах предложенной тематики. Студент выбирает вопрос, который соответствует его номеру в списке группы. Замена вопроса на другой вопрос, как и изменение его формулировки, не допускается. В том случае если Вам « не хватило» вопроса, т.е. например вопросов 26, а Ваш номер по списку 27, то нужно взять седьмой вопрос, если Ваш номер 28, то восьмой и т.д.

Работу над контрольной работой необходимо начинать с составления плана исследования, определения ключевых проблем, подлежащих изучению. Такой подход во многом облегчает определение структуры будущей работы, которая должна быть сбалансированной и иметь внутреннее единство.

Следующим важным этапом является подбор и изучение литературы по исследуемой теме. В числе основных источников следует обратить внимание на статьи в периодических изданиях, т.к. отрасль информационных технологий и систем, построенных на их основе, быстроразвивающаяся и достоверность и

актуальность отдельных положений может не соответствовать существующей действительности. Кроме того, на имеющиеся учебники, учебные пособия, монографии, справочники, нормативно- правовые документы.

Структура контрольной работы

Контрольная работа по дисциплине «Основы информационной безопасности» должна состоять из следующих разделов:

1. Титульный лист
2. Содержание
3. Введение
4. Краткая характеристика предметной области
5. Обзор законодательства
6. Модель угроз
7. Модель нарушителя
8. Рекомендации по организации системы защиты информации
9. Заключение
10. Глоссарий
11. Список литературы

Титульный лист представлен в приложении 1.

Содержание (оглавление) приводится вначале работы и включает в себя наименования структурных частей контрольной работы с указанием их начальных страниц.

Введение является вступительной частью контрольной работы, с которой начинается изложение материала. Его объем, как правило, не должен превышать 2-х страниц. Во введении следует обозначить актуальность избранной темы, указать на степень ее разработанности в трудах отечественных и зарубежных специалистов (т.н. обзор литературы), сформулировать цель и

задачи предстоящего исследования, определить круг проблем, нуждающихся в изучении.

Раздел Краткая характеристика предметной области - это сведения о специфических особенностях деятельности предприятия/организации в соответствии с индивидуальным номером варианта (Приложение 2), основных информационных потоках в этой сфере, видах и категориях обрабатываемой информации. Технические средства, участвующие в обработке информации. Общесистемные и прикладные программные средства, участвующие в обработке информации. Персонал, участвующий в обработке данных и его полномочия. Объем этого раздела 3-7 страниц.

Раздел Обзор законодательства должен содержать перечень основных законодательных актов в сфере защиты информации, нормативных документов и рекомендаций по организации системы защиты в рассматриваемой сфере деятельности. Кроме того, в этом разделе должны быть представлены краткие аннотации каждого упомянутого документа. Объем этого раздела 5-10 страниц.

Модель угроз – определяет перечень актуальных угроз. В модели угроз отражаются: непосредственно сами угрозы с указанием самых актуальных; источники угроз; общая характеристика уязвимостей; используемые средства защиты информации.

Этот раздел должен содержать информацию о возможных угрозах информационной безопасности в исследуемой предметной области, в частности: нарушения целостности, потери конфиденциальности, потери доступности; угрозы утечки информации по техническим каналам (утечка акустической, видовой) информации; угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, угроза "Анализ сетевого трафика" с перехватом передаваемой по сети информации грозы сканирования,

направленные на выявление открытых портов и служб, открытых соединений и др.; угрозы выявления паролей; угрозы внедрения ложного объекта сети; угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных; угрозы внедрения вредоносных программ, угрозы "Отказа в обслуживании"; Угрозы удаленного запуска приложений. Объем этого раздела 4-8 страниц.

Нарушитель - это лицо, предпринявшее попытку выполнения запрещенных операций по ошибке, незнанию или осознанно использующее для этого различные возможности, методы и средства. Модель нарушителя -

Модель нарушителя – содержит анализ возможностей, которыми может обладать нарушитель. Этот раздел должен содержать информацию о внутренних и внешних нарушителях; предполагаемые категории внутренний нарушителей; предполагаемые способы получения информации нарушителем; Объем этого раздела 3-7 страниц.

Рекомендации по организации системы защиты информации – на основе разработанных моделей угроз и нарушителей подготовить рекомендации по организации системы защиты информации (организационно-правовые, инженерно-технические, программно-аппаратные средства защиты).

Заключение. В заключении контрольной работы должны содержаться основные результаты проведенного исследования, а также выводы, сделанные автором на их основе. Основные результаты и выводы, подводящие итог выполненной работе, следует формулировать сжато, лаконично и аргументировано, избегая обилия общих слов и бездоказательных утверждений. Заключение, как правило, не должно превышать 2-3 страницы.

Глоссарий - это словарь узкоспециализированных терминов в области информационной безопасности и защиты информации с толкованием, используемых в контрольной работе. Объем глоссария 1-5 страниц.

Список литературы. Список использованных источников помещается в конце контрольной работы и состоит из двух частей: нормативных документов и литературы (учебники, учебные пособия, монографии, статьи в периодических изданиях, справочники, сборники, ссылки Интернет т.п.). При этом все источники нумеруются в сплошном порядке, располагаются в алфавитном порядке фамилий первых авторов или названий самих источников. При оформлении списка сведения об источниках приводятся в соответствии с правилами библиографического описания на основании ГОСТ 7.1-2003 «Библиографическая запись».

Каждую структурную часть работы (введение, основную часть, заключение, список использованных источников, приложения) следует начинать с новой страницы.

Написание контрольной работы целесообразно осуществлять последовательно (введение>основная часть>практическая часть>заключение), после глубокого и всестороннего изучения имеющейся литературы. В работе должны быть детально освещены основные вопросы исследуемой темы.

Общие требования к контрольной работе

Контрольная работа должна быть подготовлена студентом самостоятельно, иметь аналитический характер, содержать научно-исследовательские элементы. Содержание контрольной работы должно соответствовать теме, предложенной преподавателем.

Общими требованиями к контрольной работе являются: четкость и логическая последовательность изложения материала, убедительность

аргументации, краткость и ясность формулировок, исключающих неоднозначность толкования, конкретность изложения основных результатов и выводов, их научная и/или практическая значимость, обоснованность личных предположений и рекомендаций автора.

Студент **в обязательном порядке** должен **приводить ссылки** на источники, материалы из которых использованы им при написании контрольной работы. При этом в случае дословного цитирования необходимо проставление кавычек.

Оформление ссылок может осуществляться двумя путями: в виде подстрочного примечания (с проставлением верхнего индекса) и путем приведения номера согласно списку использованных источников (непосредственно в тексте в квадратных скобках). В обоих случаях автор работы обязан указывать в ссылке номер страницы, откуда заимствована та или иная информация. При оформлении ссылок в виде подстрочного примечания сведения об источнике приводятся в соответствии с правилами библиографического описания.

Контрольная работа должна быть выполнена в печатном виде. Текст контрольной работы располагается на одной стороне листа формата А 4. При этом объем контрольной работы, как правило, не должен превышать 25 страниц.

Для акцентирования внимания на определенных терминах, важных моментах, специфических особенностях, содержащихся в работе, студент может использовать шрифты разной гарнитуры (полужирный, курсив), подчеркивание и т.п.

Контрольная работа должна быть *выдержана в стиле письменной научной речи.* Прежде всего, стилю письменной научной речи характерно использование

конструкций, исключающих употребление местоимения первого лица единственного и множественного числа, местоимений второго лица единственного числа. В данном случае предполагается использовать неопределенно-личные предложения (например: «Вначале производят отбор факторов для анализа, а затем устанавливают их влияние на показатель»); формы изложения от третьего лица (например: «Автор полагает...»); предложения со страдательным залогом (например: «Разработан комплексный подход к исследованию...»).

В научном тексте нельзя использовать разговорно-просторечную лексику. Нужно использовать терминологические названия. Если есть сомнения в стилистической окраске слова, лучше обратиться к словарю.

Важнейшим средством выражения смысловой законченности, целостности и связности научного текста является использование специальных слов и словосочетаний. Эти слова позволяют отразить:

- *последовательность изложения мыслей (вначале, прежде всего, затем, во-первых, во-вторых, значит, итак);*
- *переход от одной мысли к другой (прежде чем перейти к, обратимся к, рассмотрим, остановимся на, рассмотрев, перейдем к, необходимо остановиться на, необходимо рассмотреть);*
- *противоречивые отношения (однако, между тем, в то время как, тем не менее),*
- *причинно-следственные отношения (следовательно, поэтому, благодаря этому, сообразно с этим, вследствие этого, отсюда следует, что);*

- *отношение (конечно, разумеется, действительно, видимо, надо полагать, возможно, вероятно, по сообщению, по сведениям, по мнению, по данным);*

- *итог, вывод (итак; таким образом; значит; в заключение отметим; все сказанное позволяет сделать вывод; подведя итог, следует сказать; резюмируя сказанное, отметим).*

Для выражения логической последовательности используют сложные союзы: благодаря тому что, между тем как, так как, вместо того чтобы, ввиду того что, оттого что, вследствие того что, после того как, в то время как и др. Особенно употребительны производные предлоги в течение, в соответствии с, в результате, в отличие от, наряду с, в связи с, вследствие и т.п.

В качестве средств связи могут использоваться местоимения, прилагательные и причастия (данные, этот, такой, названные, указанные, перечисленные).

В научной речи очень распространены указательные местоимения «этот», «тот», «такой». Местоимения «что-то», «кое-что», «что-нибудь» в тексте научной работы обычно не используются.

Для выражения логических связей между частями научного текста используются следующие устойчивые сочетания: приведем результаты исследования; как показал анализ; на основании полученных данных.

Для образования превосходной степени прилагательных чаще всего используются слова наиболее, наименее. Не употребляется сравнительная степень прилагательного с приставкой по- (например, повыше, побыстрее).

Особенностью научного языка является констатация признаков, присущих определяемому слову. Так, прилагательное следующие, синонимичное местоимению такие, подчеркивает последовательность перечисления особенностей и признаков (например, Рассмотрим следующие факторы,

Требования к оформлению контрольной работы.

Все страницы работы (за исключением титульного листа) должны быть пронумерованы в правом нижнем углу. При этом первой страницей является титульный лист, включаемый в общую нумерацию страниц контрольной работы.

Каждая структурная единица (содержание, введение, главы, заключение, глоссарий, список источников) должна начинаться с новой страницы, что достигается вставкой разрыва страницы. Т.о. в конце каждой структурной части электронного документа необходимо вставить разрыв страницы.

В работе должно быть создано электронное оглавление к работе (т.е. с автоматическим указателем страниц). В оглавлении должны обязательно присутствовать все структурные элементы.

В работе должен быть создан верхний колонтитул, начиная со второй страницы. Верхний колонтитул, должен содержать Фамилию Имя Отчество студента, номер группы, номер темы №n, вид работы, название дисциплины. Например:

Сидоров Валерий Петрович, группа 4410/1-1, тема № 44
Контрольная работа по дисциплине «Основы информационной безопасности»

Требования к шрифту колонтитула: Arial, размер шрифта 12, курсив, интервал междустрочный 1, выравнивание по центру.

Требования к шрифту основного текста: Times New Roman, размер шрифта 14, интервал междустрочный 1,5. Абзацный отступ 1,25. Поля: левое 3 см, остальные по 1,5 см. Выравнивание основного текста по ширине.

Требования к шрифту названий глав/параграфов. Times New Roman, размер шрифта 16, полужирный, интервал междустрочный 1,5; интервал после 6 пт. Выравнивание по центру.

Объем работы 15-25 страниц машинописного текста (без приложений).

Подготовленная и оформленная в соответствии с предъявляемыми требованиями контрольная работа с указанием даты исполнения, помещается в папку- скоросшиватель с прозрачным верхом и представляется в установленные сроки на заочное отделение для регистрации и последующей передачи преподавателю с целью ее проверки и выставления оценки. Срок предоставления работы не позднее 1 месяца до зачета.

В процессе подготовки контрольной работы студент вправе обращаться за помощью к преподавателю.

Список рекомендуемой литературы и источников

1. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации». – Собрание законодательства Российской Федерации. Издательство "Юридическая литература", 31 июля 2006, N 31, ст. 3448.
2. Приказ Федеральной налоговой службы от 21 декабря 2011 г. N ММВ-7-4/959 "Об обеспечении безопасности персональных данных при их обработке в автоматизированных информационных системах налоговых органов". – Система ГАРАНТ, 2013 г.
3. Арестова, О.Н. Комментарий к Федеральному закону от 22 декабря 2008 г. N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации" / О.Н. Арестова, Н.Н.Ковалева. – Система ГАРАНТ, 2010 г.
4. Доктрина информационной безопасности Российской Федерации. Издательство: Ось-89, 2007. – 48 с.
5. Ярочкин, В.И. Информационная безопасность. Учебник для вузов / В.И. Ярочкин. - 5-е изд. - М. : Академический проект, 2008. - 544 с. - (Gaudeamus). - ISBN 978-5-8291-0987-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=211164 (04.11.2014).
6. Основы управления информационной безопасностью : учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - М. : Горячая линия - Телеком, 2013. - 244 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 1). - библиогр. в кн. - ISBN 978-5-9912-0271-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253575 (04.11.2014).
7. Спицын, В.Г. Информационная безопасность вычислительной техники : учебное пособие / В.Г. Спицын. - Томск : Эль Контент, 2011. - 148 с. - ISBN 978-5-4332-0020-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=208694 (04.11.2014).
8. Грушо, А.А. Теоретические основы компьютерной безопасности: учеб. пособие для студ. высших учебных заведений / А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. – М.: Издательский центр «Академия», 2009. – 272 с.
9. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высших учебных заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. 3-е изд. стер. –М.: Издательский центр «Академия», 2008. –256 с.
10. Расторгуев, С.П. Основы информационной безопасности: учеб. пособие для студ. высших учебных заведений / С.П. Расторгуев. 2-е изд. стер. – М.: Издательский центр «Академия», 2009. –192 с.

11.Викторов, А.Д. Побочные электромагнитные излучения ПК и защита информации / А.Д. Викторов, В.И. Генне, Э.В. Гончаров. – Безопасность информационных технологий.- 1995, выпуск 2.- с 36.

12.Емельянов, Г.В.О Доктрине информационной безопасности Российской Федерации / Г.В. Емельянов, А.А. Стрельцов. – Информационное общество, 2007. – С. 22-24.

13. Запечников, С. В. Информационная безопасность открытых систем / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В.Ушаков. – Том 1. Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая Линия-Телеком, 2006. – 536 с.

14. Лепехин, А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты / А.Н. Лепехин. – М.: Тесей, 2008. – 176 с.

15. Лопатин, В. Н. Информационная безопасность России: Человек, общество, государство / В.Н. Лопатин. – М.: 2007. – 428 с. – Серия: Безопасность человека и общества.

16.Петренко, С. А. Политики информационной безопасности / С.А. Петренко, В.А. Курбатов – М.: Компания АйТи, 2006. – 400 с.

17.Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. – 272 с.

18.Петров В.П., Петров С.В., Информационная безопасность человека и общества : учебное пособие / Петров В.П., Петров С.В. - М. : ЭНАС, 2007. - 334 с. - ISBN 978-5-93196-814-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=42835 (04.11.2014).

19.Защита от хакеров беспроводных сетей / К. Барнс, Т. Боутс, Д. Лойд и др. ; пер. А.В. Семенов. - М. : ДМК Пресс, б.г.. - 478 с. - (Информационная безопасность). - ISBN 5-98453-012-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=85095 (04.11.2014).

20.Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. – М.: «Дашков и К», 2008. – 232 с.

Internet-ресурсы:

1. Образовательный сайт www.intuit.ru
2. Библиотека учебной и методической литературы www.window.edu.ru
3. Журнал «Открытые системы» www.osp.ru
4. Библиотека учебной и методической литературы www.ihtika.lib.ru
5. Библиотека Российской экономической академии им. Плеханова http://news.rea.ru/portal/Departments
6. Фонд Развития Интернет www.fid.ru
7. Издание о высоких технологиях http://www.cnews.ru/
8. Сайт «Лаборатории Касперского» http://www.securelist.com/ru/

9. Официальный сайт «Лаборатории Касперского» http://www.kaspersky.ru/

Приложение 1 Образец оформления титульного листа

САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ УПРАВЛЕНИЯ И ЭКОНОМИКИ

АЛТАЙСКИЙ ИНСТИТУТ ЭКОНОМИКИ

ЭКОНОМИКО-ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра экономики и менеджмента

КОНТРОЛЬНАЯ РАБОТА

по дисциплине: Основы информационной безопасности

на тему: «Обеспечение информационной безопасности в/на
……..……»
указать предметную область исследования

Вариант № XX

Выполнила студентка
Группы 19371/3-2
Иванова И.И.

Проверил:
Г.В. Грибова
_____
«___»_____
Оценка:_____

Барнаул, 2014

Приложение 2.

Примерный перечень объектов исследования

1. Налоговая инспекция
2. Отделение Пенсионного фонда
3. Комитет администрации муниципального образования
4. Коммерческий банк
5. Учреждение здравоохранения
6. Образовательное учреждение
7. Страховая организация
8. Производственное предприятие
9. Предприятие пищевой промышленности
10. Предприятие общественного питания (быстрого питания)
11. Предприятие общественного питания (ресторан)
12. Перерабатывающее предприятие (сельское хозяйство)
13. Перерабатывающее предприятие (металлургия)
14. Перерабатывающее предприятие (утилизация отходов)
15. Предприятие торговли
16. Предприятие дистрибуции
17. Транспортное предприятие
18. Складской центр
19. Логистический центр
20. Сервисный центр
21. Распределительный центр
22. Исследовательский центр
23. Выставочный центр
24. Подразделение миграционной службы
25. Издательский дом
26. Орган по стандартизации и сертификации

27. Орган по лицензированию
28. Организация сферы услуг (бытовые услуги)
29. Организация сферы услуг (медицинские услуги)
30. Организация сферы услуг (юридические услуги)

Задания, которые необходимо выполнить в ходе работы над разделами контрольной работы: *Краткая характеристика предметной области, Модель угроз, Модель нарушителя, Рекомендации по организации системы защиты информации:*

1. провести анализ информационных потоков в определенной сфере человеческой деятельности (в соответствии с индивидуальным вариантом практической части);
2. проанализировать основные угрозы безопасности в соответствии с законодательными актами и нормативными документами;
3. на основании проведенного анализа разработать модель угроз информационной безопасности, модель нарушителя с учетом особенностей рассматриваемой сферы деятельности, а также выработать рекомендации по организации системы защиты информации в этой сфере.

Дополнительные задания для студентов, отсутствовавших на установочных лекциях и/или практических занятиях.

Студенты, отсутствовавшие на установочных лекциях и/или практических занятиях дополнительно выполняют задания:

- теоретический реферативный обзор по темам лекционного материала: Понятие информационной безопасности и защита информации: организационно-правовой, аппаратно-технический, программный аспекты. Угрозы информационной безопасности, их классификация. Реферативный обзор разместить в приложении 1 к контрольной работе.
- отчет о выполненных лабораторных работ 1, 2 (разместить в приложениях 2-3)