Министерство сельского хозяйства Российской Федерации
Департамент научно-технологической политики и образования
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Красноярский государственный аграрный университет»
Институт Экономики и управления АПК

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Методические указания к комплексной лабораторной работе для студентов направления подготовки 09.03.03 – «Прикладная информатика»

Красноярск 2018

Н.В.Титовская, С.Н.Титовский

Информационная безопасность: Методические указания к комплексной лабораторной работе для студентов направления подготовки 09.03.03 – «Прикладная информатика» /Краснояр. гос. аграр. ун-т.– Красноярск, 2018. – 15 с.

Предназначены для студентов направления подготовки 09.03.03 – «Прикладная информатика» института Экономики и управления АПК.

Рецензент: Шишов В.В. профессор каф. Информационных технологий и математических методов КГТЭИ, д.т.н., профессор

Печатается по решению редакционно-издательского совета ФГБОУ ВО «Красноярский государственный аграрный университет»

ФГБОУ ВО “Красноярский государственный аграрный университет”, 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Выполнение комплексной лабораторной работы является важной составной частью в изучении дисциплины «Информационная безопасность».

Цель лабораторной работы – оценить уровень информационной безопасности на конкретном предприятии (объекте исследования) и разработать предложения для его повышения. Лабораторная работа направлена на закрепление знаний и навыков, приобретаемых при изучении дисциплины на лекциях, лабораторно-практических, индивидуальных и самостоятельных занятиях по вопросам, касающимся информационной безопасности.

Задачи лабораторной работы:

- Исследовать и проанализировать проблему, относительно обеспечения информационной безопасности объекта исследования (конкретного предприятия);
- Обозначить существующие средства защиты и их функциональные особенности;
- Выработать направления для повышения надежности хранения данных;
- Разработать программные средства, позволяющие производить защиту информации объекта исследования.

В рамках лабораторной работы все вопросы студентами решаются самостоятельно, во взаимосвязи между собой. В процессе выполнения работы необходимо изучить специальную литературу для углубления знаний по вопросам, связанных с темой работы, использовать знания, полученные при изучении других предметов, найти рациональные решения с учётом противоречивых требований.

Таким образом, выполнение работы позволяет систематизировать знания по дисциплине, учит работать со специальной литературой, расширяет кругозор студента и готовит его к дальнейшей самостоятельной работе.

1 СТРУКТУРА И СОДЕРЖАНИЕ РАБОТЫ

Предлагаемые тематики работ носят прикладной характер. По каждой теме необходимы знания следующих дисциплин: «Информатика и программирование», «Теория экономических информационных систем», «Информационные технологии», «Вычислительные системы, сети и телекоммуникации», «Базы данных», «Операционные системы, среды и оболочки», «Высокоуровневые методы информатики и программирования», «Объектно-ориентированное программирование», «Проектирование и построение баз данных», «Проектирование информационных систем», «Разработка и стандартизация программных средств и информационных технологий».

1.1. Общая структурная схема работы.

В данном разделе приведена последовательность рассмотрения вопросов, которые должны быть отражены в работе:

Введение.

1. Анализ объекта исследования.
   - 1.1. Характеристика объекта исследования.
   - 1.2. Комплекс задач, решаемых объектом исследования.
   - 1.3. Текущий уровень использования аппаратных и программных средств объекта исследования.
   - 1.4. Исследование общей безопасности предприятия.
   - 1.5. Разработка предложений по модернизации системы безопасности объекта исследования.
2. Разработка программных средств для обеспечения информационной безопасности объекта исследования.
   - 2.1. Анализ и выбор методов криптографического преобразования информации.
   - 2.2. Определение состава и назначения модулей программного обеспечения защиты информации методами криптографии.
   - 2.3. Реализация модулей.
   - 2.4. Тестирование разработанного программного обеспечения защиты информации.

2.5. Разработка эксплуатационных документов.

3. Заключение.
4. Библиографический список.
5. Приложения.

1.2. Краткое содержание разделов отчета.

Введение. Краткое обоснование актуальности темы проекта. Объект и предмет исследования. Проблема обеспечения информационной безопасности. Цель и задачи проектирования и разработки программных средств обеспечения информационной безопасности для конкретной предметной области. Методики проектирования, используемые в работе.

Раздел 1. «Анализ объекта исследования».

1.2.1. В пункте «Характеристика объекта исследования» исследуются следующие вопросы: вид деятельности предприятия, местонахождения предприятия, форма собственности, юридический статус предприятия, учредители, уставной капитал, структура товарной продукции , общая численность персонала, структура системы управления и т.д.

1.2.2. В пункте "Комплекс задач, решаемых объектом исследования" следует выделить такие как планирование производства продукции, непосредственно производство и реализация продукции, а также закупочная деятельность. В результате анализа комплекса задач, выявляются направления деятельности предприятия, которые необходимо модернизировать с точки зрения повышения информационной безопасности и защиты информации от различного рода угроз.

1.2.3. В пункте "Текущий уровень использования аппаратных и программных средств объекта исследования» должны быть отражены сведения об используемом аппаратном обеспечении: модели и технические характеристики компьютеров, периферийных устройств, топология сети (если таковая имеется), модели и характеристики сетевого оборудования; поддержка информационной безопасности и защиты информации аппаратными средствами.

Проводится исследование используемых на предприятии программных средств с точки зрения обеспечения информационной безопасности. Здесь должны быть приведены следующие сведения:

перечень программных средств; назначение программных средств; возможности программных средств; конкретные сферы применения (для каких задач используется программное обеспечение); возможности программных средств в вопросе защиты информации; достоинства и недостатки используемых программных средств по обеспечению должного уровня информационной безопасности.

1.2.4. В пункте «Исследование общей безопасности предприятия» рассматриваются вопросы, связанные с возможностью хищения, порчи информационных ресурсов предприятия (доступ в помещение, сигнализация, физические меры защиты информации, средства противопожарной охраны; доступ к информации, хранящейся в электронном виде; защита информации от несанкционированного доступа; резервное копирование данных; меры по повышению надежности и отказоустойчивости компьютерных систем; криптографические методы защиты информации; механизмы борьбы с компьютерными вирусами и т.д.).

1.2.5. В пункте "Разработка предложений по модернизации системы безопасности объекта исследования" ясно и четко формулируются предложения по усилению защиты информации на объекте исследования, выявленные в результате анализа, проведенного в пункте «Исследование общей безопасности предприятия».

Раздел 2 «Разработка программных средств для обеспечения информационной безопасности объекта исследования».

В данном разделе на основе выявленных требований разрабатывается следующее:

- Анализ и выбор методов криптографического преобразования информации. В данном пункте рассматриваются различные алгоритмы криптозащиты информации. На основе проведенного анализа выбирается наилучший алгоритм для конкретного объекта.
- Определение состава и назначения модулей программного обеспечения защиты информации методами криптографии. В данном пункте проектируется структура модулей, определяются информационные связи между модулями, проектируется интерфейс с пользователями.
- Реализация модулей. В данном пункте приводится физическая реализация проектируемого программного обеспечения защиты

информации методами криптографии. Программный код и скрипты рекомендуется включать в приложение.

- Тестирование разработанного программного обеспечения защиты информации. Тестирование является неотъемлемым компонентом жизненного цикла создания любого программно-аппаратного продукта. Тестирование программного обеспечения – это обязательный этап перед передачей программного обеспечения в эксплуатацию. Тестирование осуществляется посредством сравнения результатов выполнения алгоритмов криптозащиты с планируемыми результатами.
- Разработка эксплуатационных документов. Рекомендуется в частности включать в раздел следующие сведения:

1.Назначение и условия применения, где описывается область применения возможностей программных средств. Указываются технические средства, ОС, требования к квалификации пользователя и т.д.

2.Подготовка к работе, где указывают состав и содержание дистрибутивного носителя информации, порядок установки программы, порядок проверки работоспособности.

3.Описание операций для каждой операции обработки данных, где указывают наименование условия выполнения, подготовительные и основные действия пользователя. При этом допускаются ссылки на файлы подсказок, размещенные на магнитных носителях.

4.Аварийные ситуации, где указывают действия пользователя при отказе технических средств, несанкционированном вмешательстве в данные, обнаружении ошибок в данных.

Раздел "Эксплуатационные документы" может содержать следующие подразделы:

- руководство системного программиста;
- руководство программиста;
- руководство оператора.

Все подразделы раздела «Разработка эксплуатационных документов» оформляется в соответствии с ГОСТ 19.503-79, ГОСТ 19.504-79, ГОСТ 19.505-79.

Раздел 3. «Заключение».

Заключение должно содержать оценку результатов работы, т.е. сравнительный анализ основных технико-экономических показателей программных средств, основные выводы о новизне и практическом значении проекта.

В заключении намечаются пути и цели дальнейшей работы. Дается оценка технико-экономической эффективности, которая может быть получена при использовании результатов работы. В конце заключения указывается возможность реализации проектных решений в производстве

Раздел 4. «Библиографический список».

Список должен содержать перечень источников, использованных при выполнении работы. Источники следует располагать по алфавиту или в порядке появления ссылок на них в тексте отчета.

Сведения об источниках, включенных в список, необходимо давать в соответствии с ГОСТ 7.1-84.

Раздел 5. «Приложения»

В приложении следует включать программные разработки, а также вспомогательный материал, необходимый для полноты отчета (технологические карты, акты, справки, сложные расчеты и тому подобное).

Каждое приложение должно начинаться с нового листа с указанием в правом верхнем углу листа слова ”ПРИЛОЖЕНИЕ” прописными буквами. Приложение может иметь заголовок, который записывается симметрично тексту прописными буквами.

Если имеется больше одного приложения, их нумеруют арабскими цифрами без знака, например ПРИЛОЖЕНИЕ 2, ПРИЛОЖЕНИЕ 3 и т.д.

Нумерация страниц в приложении продолжает нумерацию страниц основного текста.

1.3. Основные требования к оформлению отчета

Текст отчета подготавливается в редакторе Word for Windows (версия 7.0 или более поздних версий) и представляются:

- в одном экземпляре для защиты;
- на дискете для последующего использования кафедрой в своей работе.

Текст следует печатать через полтора или два интервала. Минимальная высота букв не менее 2,5 мм.

Текст отчета располагается на одной стороне каждого листа белой бумаги формата А4 (210 х 297 мм.).

При подготовке текста следует заботиться о логической последовательности и четкости изложения материала; краткости и точности формулировок, исключающих возможность неоднозначного толкования; об убедительности аргументации; достоверности используемых данных и сведений; достаточности и обоснованности решений, предложений, рекомендаций и выводов.

Текст отчета должен быть четким, лаконичным, понятным.

Текст, таблицы и иллюстрационный материал следует располагать на листах, соблюдая следующие размеры полей: левое - не менее 30 мм., правое - не менее 10 мм, верхнее - не менее 20 мм, нижнее - не менее 20 мм . Формат А4. Абзацный отступ в начальной строке текста абзаца должен быть 8 мм – 12 мм. Для написания используются шрифты Times New Roman/Times new Roman Cyr, 14 pt, курсив (Italic); обычный (Normal); полужирный (Bold), с автоматической расстановкой переносов; выравнивание по ширине.

Названия различаются на 2 pt, названия самого нижнего уровня пишутся полужирно, 16 pt.

Название структурных частей отчета располагаются на отдельных строках и отделяются от текста 2-3 межстрочными интервалами, шрифт – жирный. Подчеркивать заголовки не следует.

Названия структурных частей отчета, располагаемые на отдельных строках, следует печатать симметрично тексту. Точку в конце названия структурной части ставить не нужно.

Страницы отчета необходимо нумеровать только арабскими цифрами. Нумерации подлежат все имеющиеся в отчете страницы, начиная с титульного листа. Непосредственно на титульном листе номер страницы /1/ не ставится. Последующие номера страниц проставляются в правом нижнем углу.

Пример оформления титульного листа приведен в

Приложении.

Содержание должно включать перечень всех имеющихся в тексте отчета наименований разделов, подразделов и пунктов с соответствующими номерами. Справа от наименований разделов, подразделов и пунктов отчета необходимо указывать номера страниц (листов), на которых размещается начало разделов, подразделов и пунктов по тексту отчета.

Разделы основной части нумеруются последовательно возрастающими цифрами с точкой (например, «1.», «2.», и т.д.), подразделы – в пределах своего раздела (например, «1.1.», «1.2.» и т.д.), пункты – в пределах своего подраздела (например, «1.1.1.»,
«1.1.2.» и т.д.).

При наличии в отчете чертежей формата А1 и А2, графического, и другого демонстрационного материала, на каждый из них в тексте основной части делаются соответствующие ссылки, пояснения.

Все приложения нумеруются арабскими цифрами без указания знака № (например, «Приложение 1», «Приложение 2» и т.д.). Каждое приложение следует размещать на новом листе с указанием в правом верхнем углу слова «Приложение», напечатанного жирным шрифтом. Любое из приложений должно иметь содержательный заголовок.

Список использованной литературы можно располагать в порядке появления источников в тексте отчета или в алфавитном порядке. Сведения об источниках, включенных в список, следует давать в соответствии с требованиями к описанию произведений печати в библиографических и информационных изданиях, во внутрикнижных, внутрижурнальных и статейных библиографиях.

2. ТЕМЫ РАБОТ (ПРИМЕРНЫЙ ПЕРЕЧЕНЬ).

Выбор темы, конкретизация её содержания (выбор объекта и вопросов для детальной проработки) и уточнения названия темы согласуется с руководителем.

1. Проектирование средств защиты информационной системы деканата.
2. Проектирование средств защиты информационной системы библиотеки.
3. Проектирование средств защиты для информационной системы предприятия мелкооптовой торговли.
4. Проектирование средств защиты информационной системы отдела маркетинга предприятия.
5. Проектирование средств защиты информационной системы отдела кадров предприятия.
6. Проектирование средств защиты информационной системы предприятия (по конкретному виду предприятия).
7. Проектирование средств защиты информационной системы реализации продаж в магазинах.
8. Проектирование средств защиты информационной системы для работы почтовой службы.
9. Проектирование средств защиты базы данных бухгалтерии предприятия.
10. Проектирование средств защиты информационной системы сельскохозяйственного предприятия.

3. ГРАФИК ВЫПОЛНЕНИЯ РАБОТЫ

Проверка работы руководителем и защита проводится в соответствии с установленным графиком:

График выполнения работы.

Основные этапы работы	Объём работ, %	Номер недели
1. Получение задания.		22
2. Выполнение раздела 1: Анализ объекта исследования.	50%	22-25
2.1. Характеристика объекта исследования. Комплекс задач, решаемых объектом исследования.	5%	22
2.2. Текущий уровень использования аппаратных и программных средств объекта исследования.	10%	23
2.3. Исследование общей безопасности предприятия.	20%	24
2.4. Разработка предложений по модернизации системы безопасности объекта исследования.	15%	25
3. Выполнение раздела 2: Разработка программных средств для обеспечения информационной безопасности объекта исследования.	50%	25 -34
3.1. Анализ и выбор методов криптографического преобразования информации.	5%	26
3.2. Определение состава и назначения модулей программного обеспечения защиты информации методами криптографии.	10%	27
3.3. Реализация модулей.	20%	32
3.4.Тестирование разработанного программного обеспечения защиты информации.	10%	33
3.5.Разработка эксплутационных документов	5%	34
4. Проверка и защита работы.		35, 36

4. БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Мельников,В.П., Клейменов,С.А., Петраков,А.М.. Информационная безопасность и защита информации/ Мельников,В.П., Клейменов,С.А., Петраков,А.М.. -М.: Академия, 2006. -336 с.;
2. Галатенко В.А. Основы информационной безопасности. Курс лекций.- М.: ИНТУИТ.РУ "«Интернет-Университет Информационных технологий», 2003.-280 с.
3. Милославская, Н.Г. Интрасети:обнаружение вторжений : Учеб.пособие для вузов/ Милославская, Н.Г., Толстой,А.И.. -М.: Юнити-Дана, 2001.
4. Завгородний И.В. Комплексная защита информации в компьютерных системах: Учебное пособие.-М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. - 264 с.
5. Белкин П.Ю., Михальский О.О., Проскурин В.Г. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. Пособие для вузов.- М.: Радио и связь, 1999. –168 с.
6. Проскурин В.Г., Крутов С.В. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. Пособие для вузов.- М.: Радио и связь, 2000. –168 с.
7. Галатенко В.А. Информационная безопасность: практический подход. Под ред. Бетелина В.Б. – М.: Наука, 1998.
8. Гайкович В., Першин А. Безопасность электронных банковских систем. – М.:Единая Европа, 1994.
9. Касперский Е. Компьютерные вирусы: что это такое и как с ними бороться. –М.: СК Пресс, 1998
10. Барсуков В.С. Современные технологии безопасности/ Барсуков В.С., Водолазкий В.В.. -М.: Нолидж, 2000. -496 с.
11. Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных http://www.cyberpolice.ru
12. Порталы по информационной безопасности http://infosecurity.report.ru, http://www.void.ru
13. Российский криптографический портал http://www.cryptography.ru
14. Архангельский А.Я. Программирование в Delphi 5 2-е изд., перераб. и дополн. –М.: ЗАО «издательство БИНОМ», 2000г. 1072с

Приложение 1
Образец титульного листа

Министерство сельского хозяйства Российской Федерации
Департамент научно-технологической политики и образования
Федеральное государственное бюджетное образовательное учреждение высшего образования «Красноярский государственный аграрный университет»
Институт Экономики и управления АПК
Кафедра Информационные технологии и математическое обеспечение информационных систем

Отчет по комплексной лабораторной работе по дисциплине «Информационная безопасность»

Тема:_____

Выполнил(а) студент(ка) гр. ___
_____
(Фамилия, имя, отчество)
Преподаватель_____
(должность, ФИО)

Представлен на проверку «___» _____ 20__г.
Проверен « » _____ 20__г.
Примечание_____
Оценка _____
(оценка, подпись преподавателя)

Красноярск, 20__