МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
_____ 2017 г.

Анализ заданного нормативно-правового акта Российской Федерации

Методические указания по выполнению лабораторной работы

Курск 2017

УДК 621.(076.1)
Составители: В.В. Карасовский, О.А. Демченко

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *А.Г. Спеваков*

Анализ заданного нормативно-правового акта Российской Федерации: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: В.В. Карасовский, О.А. Демченко. Курск, 2017.- 6 с., ,Библиогр.: с. 6.

Содержат сведения об администрирование и управление программно-аппаратными средствами контроля и фильтрации сетевых пакетов способах, а так же защиты от несанкционированного доступа к ресурсам персонального компьютера. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Предназначены для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ . Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Целью данной лабораторной работы является знакомство с нормативно-правовыми актами и законодательством Российской Федерации, регулирующим вопросы защиты информации.

2. ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ ЗАДАНИЯ

В ходе выполнения задания необходимо провести анализ заданного нормативного документа. После этого следует определить, какие части документа относятся к вопросам защиты информации. В справочно-поисковых системах или в сети международного информационного обмена найти комментарии к данному документу и исследовать, как менялся текст нормативного акта с момента его создания по настоящее время. По результатам анализа оформить отчет.

3. ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

Примерный перечень заданий:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (сравнить с законом Федеральный закон от 20 февраля 1995 года №24-ФЗ "Об информации, информатизации и защите информации");
2. Федеральный закон от 29.07.2004 №98-ФЗ (ред. от 24.07.2007) "О коммерческой тайне";
3. Закон РФ от 21.07.1993 №5485-1 (ред. от 18.07.2009) "О государственной тайне";
4. Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных" (сравнить версию до 2011 года и изменения, вступившие в силу после 2011 г.);
5. Федеральный закон от 06.04.2011 №63-ФЗ (ред. от 01.07.2011) "Об электронной подписи" (сравнить с законом Федеральный закон от 10 января 2002 года №1-ФЗ "Об электронной цифровой подписи");
6. Федеральный закон от 04.05.2011 №99-ФЗ (ред. от 19.10.2011, с изм. от 21.11.2011) "О лицензировании отдельных видов деятельности" (сравнить с законом Федеральный закон от 8

августа 2001 года № 128-ФЗ «О лицензировании отдельных видов деятельности»);

7. Постановление Правительства РФ №608 от 26.06.95 г. «О сертификации средств защиты информации» (сравнить с законом Закон РФ от 10.06.1993 №5151-1 "О сертификации продукции и услуг");

8. Федеральный закон от 28.12.2010 №390-ФЗ "О безопасности" (сравнить с законом Закон Российской Федерации от 5 марта 1992 года №2446-1 "О безопасности");

9. Постановление Правительства РФ от 15.08.2006 №504 (ред. от 24.09.2010) "О лицензировании деятельности по технической защите конфиденциальной информации";

10. Постановление Правительства РФ от 31.08.2006 №532 (ред. от 24.09.2010) "О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации";

11. Приказ ФСБ РФ №416, ФСТЭК РФ №489 от 31.08.2010 "Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования".

4. СОДЕРЖАНИЕ ОТЧЁТА

1. титульный лист;
2. цель работы;
3. назначение нормативно-правового акта
4. выдержки из статей нормативно-правового акта, касающиеся вопросов защиты информации с комментариями;
5. менялся ли документ и в чем? Предположите, с чем были связаны эти изменения.
6. выводы по проделанной работе.

5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие части документа относятся к вопросам защиты информации?
2. Что показывают комментарии к данному документу?
3. Как менялся текст нормативного акта с момента его создания по настоящее время?

6. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Справочно-поисковая система «Консультант Плюс» [Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.consultant.ru/

2. Справочно-поисковая система «Гарант» [Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.garant.ru/

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
_____ 2017 г.

Определение класса государственной информационной системы (ГИС)

Методические указания по выполнению практической работы

Курск 2017

УДК 621.(076.1)
Составители: Е.С. Волокитина, М.О. Таныгин.

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *А.Г. Спеваков*

Определение класса государственной информационной системы (ГИС): методические указания по выполнению практической работы / Юго-Зап. гос. ун-т; сост.: Е.С. Волокитина, М.О. Таныгин.. Курск, 2017.- 12 с.: ил.3,табл. 1 ,Библиогр.: с. 12.

Содержат сведения об администрирование и управление программно-аппаратными средствами контроля и фильтрации сетевых пакетов способах, а так же защиты от несанкционированного доступа к ресурсам персонального компьютера. Указывается порядок выполнения практической работы, правила оформления и содержание отчета.

Предназначены для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ . Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Научиться определять класс государственной информационной системы (ГИС).

2. ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ ЗАДАНИЯ:

Ознакомиться и изучить основные принципы разработки организационно-правовых аспектов деятельности службы защиты информации.

3. ЗАДАНИЕ НА ПРАКТИЧЕСКУЮ РАБОТУ

1. В соответствии с предложенным вариантом организации или предприятия проанализировать организационно-правовое обеспечение защиты информации в системе деятельности предприятия в целом.
2. Выявить существующие проблемные моменты и узкие места.
3. В соответствие с Законом "Об информации, информатизации и защите информации", Законом Российской Федерации "О безопасности" описать основные подходы к разработке организационно-правового обеспечения службы защиты информации на выбранном предприятии.
4. Определить круг задач службы зашиты информации (СЗИ).
5. Сформулировать основные функции СЗИ.
6. Выделить в организационно-штатной структуре штатные единицы, обеспечивающие реализацию данных функции и особенности взаимодействия между собой.
7. Проанализировать нормативное обеспечение деятельности СЗИ, выявить проблемы.
8. Сформировать общую структуру нормативной документации по обеспечению безопасности информации в организации в следующей иерархии:

- Документы концептуального уровня, которые должны быть разработаны руководителями организаций;
- Документы общего уровня (применения);

- Документы, регламентирующие работу персонала с защищаемыми носителями.

9. Разработать отсутствующие документы, опираясь на законодательную базу, указанную в списке литературы, а также, используя Гарант, Консультант-Плюс. Доработать несоответствующие требованиям законодательства документы.

Разработать:

1) Положение о подразделении по защите информации. Общее руководство по руководству, функциям, задачам, правам, обязанностям, ответственности и штатной структуре.

2) Положение о категорировании ресурсов.

4. ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1. Какие функции выполняет СЗИ предприятия для решения задач защиты информации?
2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
3. Какова специфика организации и выполнения охранных функций?
4. Каковы суть и содержание нормативной основы организации ЗСИ?
5. Какие факторы влияют на формирование организационно-правового обеспечения защиты информации?
6. Какова структура организационно-правовой основы защиты информации?
7. Опишите организационно-правовые мероприятия по защите конфиденциальной информации.

5. ТЕОРИТИЧЕСКИЕ СВЕДЕНИЯ

Защита информационных ресурсов реализуется в рамках нескольких направлений деятельности СЗИ. Это решение научно-технических проблем, правовое регулирование отношений в процессе информатизации деятельности любой организации.

Разработка организационно-правового обеспечение защиты информации является актуальной в связи с признанием за

информацией статуса товара, продукта общественного производства, установления в законодательном порядке права собственности на информацию.

Такая постановка вопроса приобретает особый смысл и характер в условиях демократизации общества, формирования рыночной экономики, включения нашего государства в мировое экономическое сообщество. Если решение вопросов развития производственной базы создания средств информатики в какой-то мере можно осуществить с использованием рыночных структур и отношений, то разработка и внедрение законодательной базы информатизации невозможны без активной государственной информационной политики, направленной на построение по единому замыслу организационно-правового механизма управления информационными процессами» увязанного с научно-технической базой информатизации.

Организационно-правовое обеспечение является многоаспектным понятием, включающим законы, решения, нормативы и правила, организационно-распорядительные мероприятия.

Применительно к защите информации, обрабатываемой в информационной системе, данный вид обеспечения имеет ряд принципиальных специфических особенностей, обусловленных следующими факторами, которые показаны на рисунке 1.1.

Рис. 1.1. Факторы, влияющие на формирование организационно-

правового обеспечения защиты информации

Исходя из приведенных обстоятельств, комплекс вопросов, решаемых организационно-правовым обеспечением, может быть сгруппирован в три класса:

− организационно-правовая основа защиты информации в информационных системах;

− технико-математические аспекты организационно-правового обеспечения;

− юридические аспекты организационно-правового обеспечения защиты.

Организационно-правовая основа защиты информации должна включать (таблица 1.1).

Таблица 1.1

Структура организационно-правовой основы защиты информации

№ п/п	**Формирующие составляющие организационно-правовой основы защиты информации в службе защиты информации**
1	Определение подразделений и лиц, ответственных за организацию защиты информации
2	Нормативно-правовые, руководящие и методические материалы (документы) по защите информации
3	Меры ответственности за нарушение правил защиты
4	Порядок разрешения спорных и конфликтных ситуаций по вопросам защиты информации

Под технико-математическими аспектами организационно-правового обеспечения понимается совокупность технических средств, математических методов, моделей, алгоритмов и программ, с помощью которых в ИС могут быть соблюдены все условия, необходимые для юридического разграничения прав и ответственности относительно регламентов обращения с защищаемой информацией. Основными из этих условий являются следующие:

− фиксация на документе персональных идентификаторов ("подписей") лиц, изготовивших документ и (или) несущих ответственность за него;

− фиксация (при любой необходимости) на документе

персональных идентификаторов (подписей) лиц, ознакомившихся с содержанием соответствующей информации;

− невозможность незаметного (без оставления следов) изменения содержания информации даже липами, имеющими санкции на доступ к ней,

− т.е. фиксация фактов любого (как санкционированного, так и несанкционированного) изменения информации;

− фиксация факта любого (как несанкционированного, так и санкционированного) копирования защищаемой информации.

Под юридическими аспектами организационно-правового обеспечения защиты информации в ИС понимается совокупность законов и других нормативно-правовых актов, с помощью которых достигаются следующие цели;

− устанавливается обязательность соблюдения всеми лицами, имеющими отношение к информационной системе всех правил защиты информации;

− узакониваются меры ответственности за нарушение правил защиты;

− узакониваются технико-математические решения вопросов организационно-правового обеспечения защиты информации;

− узакониваются процессуальные процедуры разрешения ситуаций, складывающихся в процесс: функционирования систем защиты.

Таким образом, вся совокупность вопросов, возникающих при решении проблем организационно-правового обеспечения, может быть представлена в виде схемы, приведенной на рис.1.2.

Рис. 1.2. Структура Организационно-правового обеспечения защиты информации, формируемого в службе защиты информации

Основополагающим понятием в области правового аспекта защиты информации является “информация”. Закон РФ “Об информации, информатизации и защите информации” определяет понятие информация как “сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления”.

При решении организационно-правовых вопросов обеспечения информационной безопасности исходят из того, что информация подпадает под нормы вещного права, что дает возможность применять к информации нормы Уголовного и Гражданского права в полном объеме.

Анализ организационно-правового обеспечения планируемых к осуществлению мероприятий в области организации защиты информации всегда должен предшествовать принятию окончательного решения о реализации этих мероприятий.

К организационно-правовым мероприятиям по защите конфиденциальной информации относятся мероприятия по разработке и принятию определенных документов предприятий и организаций, регламентирующих степень и порядок допуска

собственных сотрудников, а также сторонних лиц и организаций к конкретным информационным ресурсам.
Организационно-правовая защита информации реализуется путем установления на предприятии режима конфиденциальности.
Можно выделить три формы конфиденциальных отношений, что представлено в таблице 1.2.

Таблица 1.2

Формы конфиденциальных отношений

Субъекты отношений	Реализация отношений
Между сотрудником предприятия и самим предприятием как юридическим лицом	Реализуется на практике путем составления соответствующего трудового договора или контракта, заключаемого с сотрудником предприятия
Складывающиеся между конкретным сотрудником и другими сотрудниками этого предприятия	Эти отношения развиваются как по вертикали, так и по горизонтали. Указанные отношения называются конфиденциальными отношениями по служебным функциям. Юридически эти отношения закрепляются многообразными административно-правовыми решениями, например приказами о выполнении определенных работ, и регламентируются "Должностными инструкциями"
Складывающиеся в рамках хоздоговорных работ и базирующиеся на договоре между партнерами	Юридически конфиденциальные отношения закрепляется в виде четко сформулированных требований и обязательств, которые выдвигают договаривающиеся стороны, и фиксируют в договоре

В вопросах реализации технических мероприятий обеспечения информационной безопасности с точки зрения правового обеспечения основное внимание следует уделять выполнению требований лицензирования исполнителей работ и использования сертифицированных средств защиты, а также действующим ограничениям на применение специальных технических средств.
В существующей практике можно выделить следующие основные аспекты решения проблемы защиты информации:
- анализ правового обеспечения;
- реализация организационно-правовых мероприятий защиты;
- реализация технических мероприятий по защите информации.

Комплексное изучение установленных норм и правил в конкретной прикладной области всегда является обязательным элементом

культуры работающего в этой области специалиста.

6. ХОД РАБОТЫ

1. В соответствии с предложенным вариантом организации или предприятия проанализировать организационно-правовое обеспечение защиты информации в системе деятельности предприятия в целом.

- Государственная организация
- Образование
- Здравоохранение
- другие
- Частная организация

2. Выявить существующие проблемные моменты и узкие места.

3. В соответствие с Законом "Об информации, информатизации и защите информации", Законом Российской Федерации "О безопасности" описать основные подходы к разработке организационно-правового обеспечения службы защиты информации на выбранном предприятии.

4. Определить круг задач службы зашиты информации (СЗИ).

5. Сформулировать основные функции СЗИ.

6. Выделить в организационно-штатной структуре штатные единицы, обеспечивающие реализацию данных функции и особенности взаимодействия между собой.

7. Проанализировать нормативное обеспечение деятельности СЗИ, выявить проблемы.

8.Сформировать общую структуру нормативной документации по обеспечению безопасности информации в организации в следующей иерархии:

- Документы концептуального уровня, которые должны быть разработаны руководителями организаций;
- Документы общего уровня (применения);
- Документы, регламентирующие работу персонала с защищаемыми носителями.

9. Разработать отсутствующие документы, опираясь на законодательную базу, указанную в списке литературы, а также,

используя Гарант, Консультант-Плюс. Доработать несоответствующие требованиям законодательства документы.

Разработать:

1) Положение о подразделении по защите информации. Общее руководство по руководству, функциям, задачам, правам, обязанностям, ответственности и штатной структуре.

2) Положение о перечне ресурсов.

7. СПИСОК КОНТРОЛЬНЫХ ВОПРОСОВ

1. Какие функции выполняет СЗИ предприятия для решения задач защиты информации?
2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
3. Какова специфика организации и выполнения охранных функций?
4. Каковы суть и содержание нормативной основы организации ЗСИ?
5. Какие факторы влияют на формирование организационно-правового обеспечения защиты информации?
6. Какова структура организационно-правовой основы защиты информации?
7. Опишите организационно-правовые мероприятия по защите конфиденциальной информации.

8. БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Справочно-поисковая система «Консультант Плюс» [Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.consultant.ru/
2. Справочно-поисковая система «Гарант» [Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.garant.ru/

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
_____ 2017 г.

Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации

Методические указания по выполнению практической работы

Курск 2017

УДК 621.(076.1)
Составители: Е.С. Волокитина, М.О. Таныгин.

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *А.Г. Спеваков*

Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации: методические указания по выполнению практической / Юго-Зап. гос. ун-т; сост.: Е.С. Волокитина, М.О. Таныгин.. Курск, 2017.- 7 с.: ил.3, табл.: 1,Библиогр.: с. 7.

Содержат сведения об администрирование и управление программно-аппаратными средствами контроля и фильтрации сетевых пакетов способах, а так же защиты от несанкционированного доступа к ресурсам персонального компьютера. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Предназначены для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ . Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Разработать структуру государственных стандартов Российской Федерации в области информационной безопасности и защиты информации.

2. ЗАДАНИЕ НА ПРАКТИЧЕСКУЮ ПАБОТУ

Ознакомиться с принципами системного подхода при создании структуры ГОСТ и ИСО.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Произвести поиск всех существующих государственных и международных стандартов в области информационных технологий, информационной безопасности и защиты информации. При нахождении – вносить в универсальный каталогизатор дисков, файлов, папок, а также любых нефайловых элементов wincatalog[1].

Пример заполнения приведен на рисунке 1.

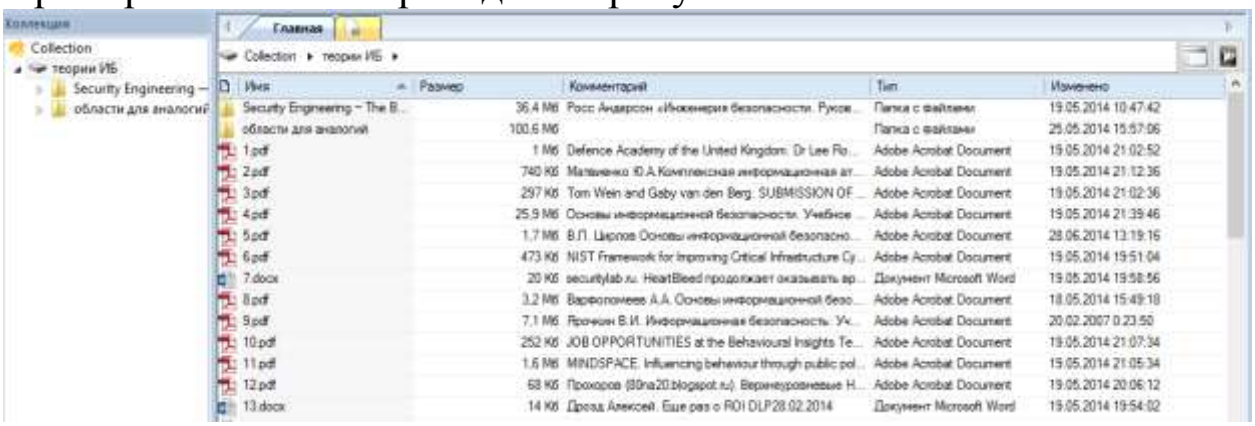

Рис.1 – Пример внесения документов в универсальный каталогизатор

2. При заполнении присваивать теги, которые описывают данный документ или область его применения, для последующей группировки.

[1] http://www.wincatalog.com/ru/

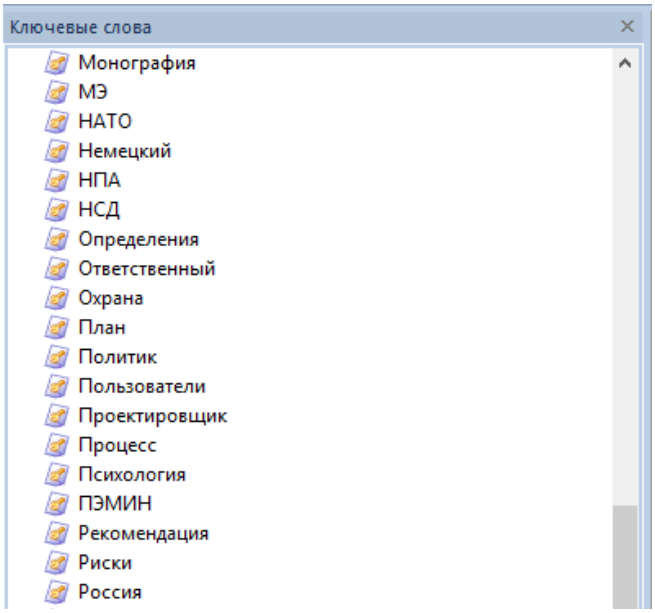

Рис.2 – Пример создания списка тегов

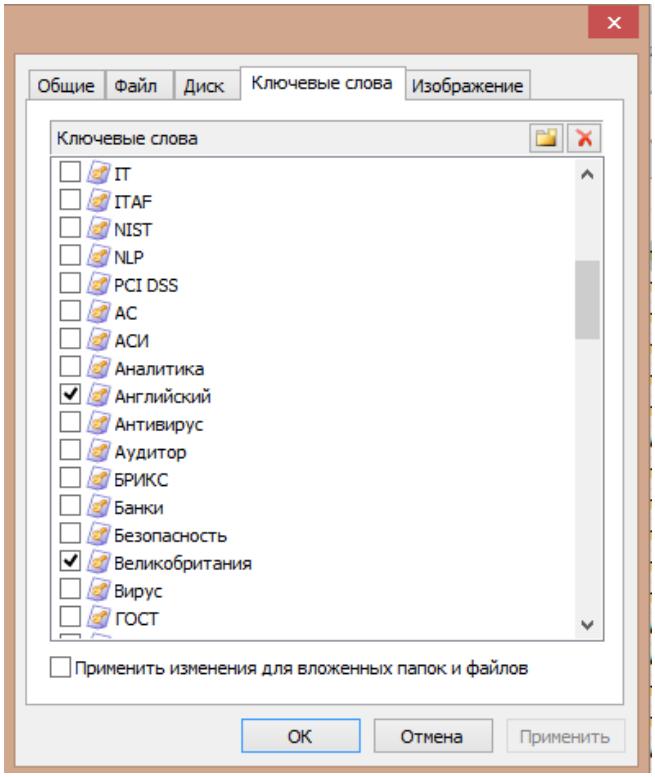

Рис.3 – Пример присваивания тегов документу

3. После заполнения системы тегов – необходимо графически их представить с помощью программы FreeMind[2] или аналога.

[2] http://sourceforge.net/projects/freemind/

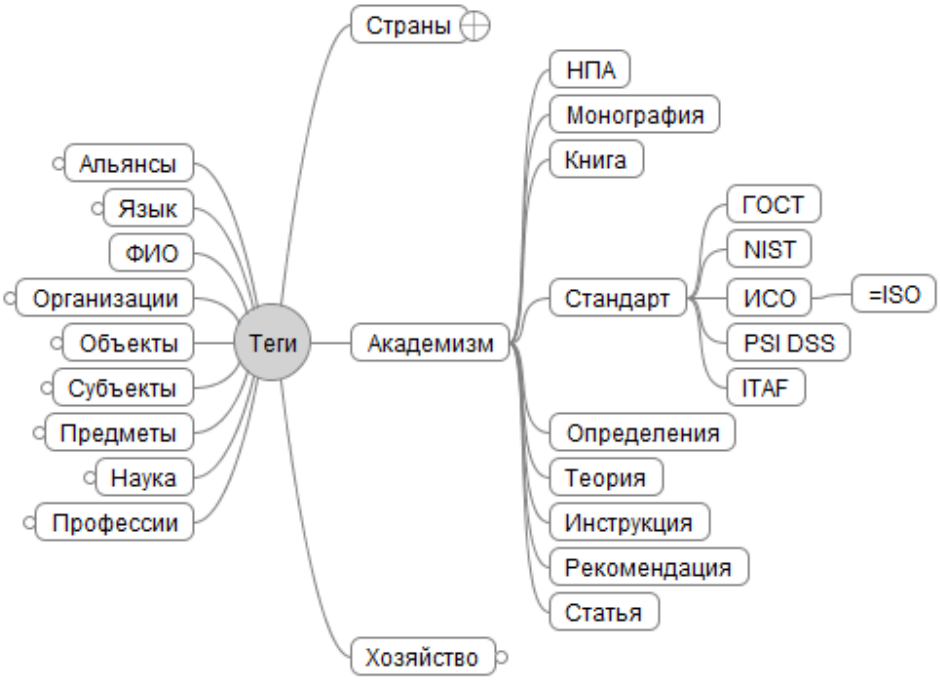

Рис.4 – Пример графического представления тегов

4. На основе полученных данных - заполнить таблицу с перечнем найденных ГОСТ и ИСО по приведенному примеру:

Таблица 1 – Список стандартов

№ п/п	Номер стандарта	Статус
Защита сетей общего пользования		
1.	ГОСТ Р 53110-2008	Действует
2.	ГОСТ Р 53111-2008	Действует
3.	ГОСТ Р 53109-2008	Действует
Оценка безопасности автоматизированных систем		
4.	ГОСТ Р ИСО/МЭК ТО 19791-2008	Действует
5.		

5. Составить отчет. В отчете должны быть представлены четко видные и понятные скрины экрана при выполнении работы и оформленная таблица.

6. Найти нужно как можно больше стандартов.

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Дать полное определение ГОСТ
2. Дать полное определение ИСО
3. Заполнить таблицу №1

4. СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Справочно-поисковая система «Консультант Плюс» [Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.consultant.ru/
2. Справочно-поисковая система «Гарант»[Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.garant.ru/
3. Справочно-поисковая система«Федеральное агентство по техническому регулированию и метрологии» [Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.gost.ru/wps/portal/
4. Справочно-поисковая система«Международная организация по стандартизации» [Электронный ресурс]: - Электрон. дан. - Режим доступа: www.iso.org

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
_____ 2017 г.

Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности

Методические указания по выполнению практической работы

Курск 2017

УДК 621.(076.1)
Составители: Е.С.Волокитина,М.О. Таныгин.

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *А.Г. Спеваков*

Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности: методические указания по выполнению практической работы / Юго-Зап. гос. ун-т; сост.: Е.С.Волокитина,М.О. Таныгин. Курск, 2017.- 7 с.: табл. 2, ,Библиогр.: с. 7.

Содержат сведения об администрирование и управление программно-аппаратными средствами контроля и фильтрации сетевых пакетов способах, а так же защиты от несанкционированного доступа к ресурсам персонального компьютера. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Предназначены для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ . Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Целью данной лабораторной работы является обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.

2. ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ ЗАДАНИЯ

В ходе выполнения задания необходимо провести анализ сертифицированных продуктов в заданной области информационной безопасности. После этого следует определить, какие средства защиты являются наиболее приемлемыми для использования в системах защиты. По результатам анализа оформить отчет.

При поиске средств защиты в заданной области, искать сертификацию на соответствие требованиям:

№	Вид СЗИ	Предназначение средства (область применения)
1.	Средства защиты от несанкционированного доступа	соответствует документу «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа»
2.	Межсетевые экраны	соответствует документу «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатель защищенности от несанкционированного доступа к информации»
3.	Антивирусные средства	соответствует документу «Требования к средствам антивирусной защиты»

№	Вид СЗИ	Предназначение средства (область применения)
		соответствует документу «Профиль защиты средств антивирусной защиты»
4.	Средства криптографической защиты	«может использоваться для криптографической защиты»
5.	Средства обнаружения вторжений	соответствует документу «Требования к системам обнаружения вторжений»
		соответствует документу «Профиль защиты систем обнаружения вторжений уровня узла»
6.	Средства контроля защищенности (автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированных систем)	«является средством анализа защищенности и обнаружения уязвимостей»
7.	Средства резервного копирования	«предназначен для создания автоматизации процессов резервного копирования»

3. ЗАДАНИЕ НА ПРАКТИЧЕСКУЮ РАБОТУ

1. Определить, кто из регуляторов проводит сертификацию в заданной области средств защиты информации

2. Пользуясь сайтами регуляторов в области защиты информации Федеральной службы безопасности (http://clsz.fsb.ru/) и Федеральной службы по техническому и экспортному контролю (http://fstec.ru/) выбрать средства защиты по направлению (номер в списке группы по порядку):

2.1. Средства защиты от несанкционированного доступа;

2.2. Межсетевые экраны;

2.3. Антивирусные средства;
2.4. Средства криптографической защиты;
2.5. Средства обнаружения вторжений;
2.6. Средства контроля защищенности;
2.7. Средства резервного копирования;
2.8. Свой вариант (по согласованию).

3. Сделать сравнительный анализ всех средств защитыв форме таблицы.

№	Название	Срок действия	Выполняемые функции	Изготовитель

4. Из полученного списка и определить наиболее привлекательные средства защиты. Объяснить почему.

5. Найти сертификаты для выбранных средств защиты информации (на сайтах производителей).

6. Сопоставить данные из сертификата выбранного средства защиты и требования руководящего документа Гостехкомисии или другого соответствующего документа (найти ссылку в сертификате).

4. ТРЕБОВАНИЯ К ОТЧЕТУ

Отчет должен содержать:

1. титульный лист;
2. цель работы;
3. заданную область информационной безопасности;
4. сравнительный анализ средств защиты;
5. выбранное оптимальное средство защиты, обоснование почему и сертификат на него (скачать на сайте производителя СЗИ);
6. Перечень документов, на соответствие которым сертифицирован продукт;
7. выводы по проделанной работе.

5. СПИСОК КОНТРОЛЬНЫХ ВОПРОСОВ

1. Как проводится сертификация средств защиты информации?
2. Что показывают характеристики данного средства защиты?
3. Какой регулятор контролирует данную область информационной безопасности?
4. Какая основная информация содержится в сертификате?

6. СПИСОК ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

1. Справочно-поисковая система «Консультант Плюс» [Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.consultant.ru/
2. Справочно-поисковая система «Гарант» [Электронный ресурс]: - Электрон. дан. - Режим доступа: http://www.garant.ru/
3. Информационный ресурс «Центр по лицензированию, сертификации и защите государственной тайны ФСБ России» [Электронный ресурс]: - Электрон. дан. - Режим доступа: http://clsz.fsb.ru/
4. Информационный ресурс «ФСТЭК России» [Электронный ресурс]: - Электрон. дан. - Режим доступа:http://fstec.ru/