

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 08.09.2017 16:34:33
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

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

г.

Оглавление

Цель работы:	3
1. Требования к выполнению задания:	3
2. Задание:	3
3. Теория.....	4
4. Ход работы:	8
5. Вопросы.....	9
Список дополнительной литературы:	9

Цель работы:

научиться определять класс государственной информационной системы (ГИС).

1. Требования к выполнению задания:

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

2. Задание:

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 защиты 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.

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.

3. Теория

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 обеспечения 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.

4. 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 соответствии 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 защиты 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.

5. Вопросы

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.

Список дополнительной литературы:

1. Справочно-поисковая система «Консультант Плюс»;
2. Справочно-поисковая система «Гарант»