Министерство образования и науки РФ

Государственное образовательное учреждение высшего профессионального образования

**«Санкт-Петербургский государственный электротехнический университет “ЛЭТИ” им. В.И. Ульянова (Ленина)» (СПбГЭТУ)**

РАБОЧАЯ ПРОГРАММА

дисциплины

*«Организационное и правовое обеспечение информационной безопасности»*

Для подготовки дипломированных специалистов по специальности 090301.65

*«Компьютерная безопасность»*

Санкт-Петербург

2011

Санкт-Петербургский государственный электротехнический

университет “ЛЭТИ”

"УТВЕРЖДАЮ"

проректор по учебной работе

Лысенко Н.В.

"\_\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_2011 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

*«Организационное и правовое обеспечение информационной безопасности»*

Для подготовки дипломированных специалистов по специальности 090301.65

*«Компьютерная безопасность»*

Уч.план № 836

Факультет компьютерных технологий и информатики

Кафедра автоматизированных систем обработки информации и управления

Курс – 5

Семестр – 10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 54 ч. |  | Дифференцированный зачет | 10 семестр |
|  |  |  |  |  |
| Практические занятия | 18 ч. |  |  |  |
|  |  |  |  |  |

|  |  |
| --- | --- |
| Аудиторные занятия | 72 ч. |
| Самостоятельные занятия | 30 ч. |
| Всего часов | 102 ч. |

2011 г.

Рабочая программа обсуждена на заседании кафедры fвтоматизированных систем обработки информации и управления «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2011 г., протокол № \_\_\_\_.

Рабочая программа составлена в соответствии с государственным образовательным стандартом для дипломированных специалистов по специальности

090301.65 — «Компьютерная безопасность»

Дисциплина «Организационное и правовое обеспечение информационной безопасности» преподается на основе изученных ранее дисциплин:

* Основы информационной безопасности.;
* Правоведение.

и обеспечивает выполнение ВКР.

Рабочая программа одобрена методической комиссией факультета компьютерных технологий и информатики «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2011 г.

Аннотация дисциплины

Учебная дисциплина «Организационное и правовое обеспечение информационной безопасности» («ОПО ИБ») является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Она призвана обеспечить освоение слушателями практических навыков работы с нормативно-правовой базой деятельности в области обеспечения информационной безопасности автоматизированных систем.

**Цели и задачи дисциплины**

Изучение дисциплины направлено на формирование знаний об организационных и правовых аспектах обеспечения информационной безопасности, а также на формирование практических навыков работы с нормативно-правовой базой в данной области.

**Требования к уровню освоения дисциплины**

Изучение дисциплины направлено на формирование вклада в следующие компетенции:

*ОК-5* – способность понимать социальную значимость своей будущей профессии, цели и смысл гос.службы, обладать высокой мотивацией к выполнению проф.деятельности в области обеспечения ИБ и защиты интересов личности, общества и государства, готовность и способность к активной состязательной деятельности в условиях информационного противоборства;

*ПК-5* – способность использовать нормативные правовые документы в своей профессиональной деятельности;

*ПК-14* – способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем;

*ПК-31* – способность разрабатывать оперативные планы работы первичных подразделений;

*ПК-33* – способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере проф. деятельности;

*ПСК-8.7* – способность разрабатывать проекты нормативных и правовых актов предприятия, учреждения, организации, регламентирующих деятельность по обеспечению ИБ ОИ на базе КС в защ.исполнении.

В результате изучения дисциплины студент должен

знать:

* основы комплексного обеспечения информационной безопасности;
* основы правового обеспечения информационной безопасности;
* основные положения законодательства РФ в области информационной безопасности;

уметь:

* применять действующую законодательную базу в области обеспечения компьютерной безопасности;
* отыскивать необходимые нормативные правовые акты и отдельные информационно-правовые нормы в системе действующего законодательства, в том числе с помощью справочно-поисковых систем правовой информации;
* разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;

владеть:

* системным подходом к организации защиты информации;
* навыками работы с нормативными правовыми актами
* навыками организации и обеспечения режима секретности и организации пропускного и внутриобъектового режима.

Содержание рабочей программы

**Раздел I. Правовое обеспечение ИБ**

**1.1. Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности**

Структура информационной сферы и характеристика ее элементов. Информация как объект правоотношений.Категории информации по условиям доступа к ней и распространения. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.

Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации Понятие и виды защищаемой информации по законодательству РФ. Перспективы развития законодательства в области информационной безопасности.

**1.2. Правовой режим защиты государственной тайны**

Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Организационные меры, направленные на защиту государственной тайны. Порядок допуска и доступа к государственной тайне. Иные меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны). Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

**1.3. Правовые режимы защиты конфиденциальной информации**

Понятие «конфиденциальной» информации по российскому законодательству. Основные виды «конфиденциальной» информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна. Правовые режимы «конфиденциальной» информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации.

Юридическая ответственность за нарушения правовых режимов конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).

**1.4. Лицензирование и сертификация в области защиты информации**

Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности.

Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.

**1.5. Правовая охрана результатов интеллектуальной деятельности**

Законодательство РФ об интеллектуальных правах. Интеллектуальные права: понятие, виды.

Авторское право. Объекты и субъекты авторского права. Исключительные авторские права. Правовая охрана программ для ЭВМ, баз данных, топологий интегральных микросхем и единых технологий. Лицензии операционных систем (Unix, Linux, Windows). Защита интеллектуальных прав.

**1.6. Преступления в сфере компьютерной информации**

Преступления в сфере компьютерной информации. Признаки и элементы состава преступления. Криминалистическая характеристика преступлений в сфере компьютерной информации. Расследование преступлений в сфере компьютерной информации. Особенности основных следственных действий. Криминалистические аспекты проведения расследования. Сбор доказательств. Экспертиза преступлений в сфере компьютерной информации. Проблемы судебного преследования за преступления в сфере компьютерной информации.

**1.7. Нормы международного права в информационной сфере**

Понятие международного информационного обмена. Законодательство РФ об участии в международном информационном обмене. Правовой режим участия в международном обмене. Субъекты и объекты международного информационного обмена. Международное право в сфере телекоммуникаций и связи. Международно-правовые нормы в деятельности средств массовой информации.

Международно-правовые аспекты защиты прав и свобод личности в связи с применением современных информационных технологий.

Международное сотрудничество в области борьбы с преступностью в сфере высоких технологий.

**Раздел 2. Организационное обеспечение информационной безопасности**

**2.1. Понятие системы защиты информации**

Модели систем и процессов обеспечения информационной безопасности. Анализ и оценка угроз информации. Понятие системы защиты информации. Анализ риска. Защита информации от стихийных бедствий. Наводнение. Землетрясение. Ураган. Противопожарная защита. Отключение коммуникаций: электроэнергия, канализация, газ, телефон, вода, каналы связи.

**2.2. Методы обеспечения физической безопасности**

Объекты обеспечения физической безопасности: сооружения, предметы, люди. Проектирование здания. Охрана территории. Охрана здания. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения. Безопасность при транспортировке носителей информации. Личная безопасность сотрудников и членов их семей. Защита документов от подделок. Обнаружение фальсификации документов. Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства. Физическая защита неподвижных объектов. Пропускной режим.

**2.3. Технологические меры поддержания безопасности**

Проблема безопасности технологии. Организация работы персонала. Резервирование оборудования и дублирование информации. Система инструкций и правил. Администрирование технологического процесса. Контроль доступа и средства поиска и досмотра. Системы контроля доступа.

**2.4. Организация режима секретности**

Виды представления информации. Пути прохождения информации. Учет получения, перемещения, преобразования, хранения и уничтожения информации. Секретариаты. Первые отделы. Служба собственной безопасности. Категорирование объектов. Подбор и расстановка кадров.

#### **Перечень практических занятий**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование темы занятия | Номер темы | Трудоемкость |
| 1 | Правовые режимы защиты информации | 1.2,1.3 | 9 |
| 2 | Лицензирование и сертификация | 1.4 | 5 |
| 3 | Преступления в сфере компьютерной информации | 1.6 | 4 |

**Распределение учебных часов по темам, видам занятий**

**и видам самостоятельной работы**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  темы | Название разделов и тем | Объем учебных часов | | | | | | | Семестр | Литература по темам |
| Лекции | Лабор.  занят. | Практ.занят. | Аудит.  занят. | | Сам.  работа | Всего |
| Всего | в т.ч. инт.формы |
| 1.1 | Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности | 4 |  |  | 4 |  |  | 4 | 10 | Л1, Л2, Л5 |
| 1.2 | Правовой режим защиты государственной тайны | 4 |  | 4 | 7 | 4 | 4 | 11 | 10 | Л1, Л2, Л5, Д1 |
| 1.3 | Правовые режимы защиты конфиденциальной информации | 8 |  | 5 | 12 | 5 | 4 | 16 | 10 | Л1, Л2, Л5,Д1 |
| 1.4 | Лицензирование и сертификация в области защиты информации | 4 |  | 5 | 8 | 5 | 4 | 12 | 10 | Л1, Л2, Л5 |
| 1.5 | Правовая охрана результатов интеллектуальной деятельности | 8 |  |  | 12 |  | 4 | 16 | 10 | Л1, Л2, Л5, Д1, Д3 |
| 1.6 | Преступления в сфере компьютерной информации | 8 |  | 4 | 11 | 4 | 4 | 15 | 10 | Л1, Л2, Л5, Д2, Д3 |
| 1.7 | Нормы международного права в информационной сфере | 4 |  |  | 4 |  | 2 | 6 | 10 | Л1, Л2, Л5 |
| 2.1 | Понятие системы защиты информации | 4 |  |  | 4 |  | 2 | 6 | 10 | Л1, Л2, Л3, Л4 |
| 2.2 | Методы обеспечения физической безопасности | 4 |  |  | 4 |  | 2 | 6 | 10 | Л1, Л2, Л3, Л4 |
| 2.3 | Технологические меры поддержания безопасности | 4 |  |  | 4 |  | 2 | 6 | 10 | Л1, Л2, Л3, Л4 |
| 2.4 | Организация режима секретности | 2 |  |  | 2 |  | 2 | 4 | 10 | Л1, Л2, Л3, Л4 |
| ИТОГО: | | 54 |  | 18 | 72 | 18 | 30 | 102 |  |

**Учебно-методическое обеспечение дисциплины**

# Основная литература

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Название, библиографическое описание | Л | Лр | Пз (С) | Кп | Кр | К-во экз. в библ. (на каф.) | Гриф |
| **Л1** | Малюк, А. А. Информационная безопасность: концептуальные и методологичесские основы защиты информации : учеб. пособие для вузов / А. А. Малюк. - М. : Горячая линия-Телеком, 2004. | 10 |  | 10 |  |  | нет |  |
| **Л2** | Ярочкин, В. И. Информационная безопасность : учеб. для вузов / В. И. Ярочкин. - 4-е изд. - М. : Академ. проект, 2006. | 10 |  | 10 |  |  | нет |  |
| **Л3** | Основы организационного обеспечения информационной безопасности объектов информатизации : учеб. пособие / С. Н. Сёмкин, Э. В. Беляков, С. В. Гребнев, В. И. Козачок. - М. : Гелиос АРВ, 2005. | 10 |  |  |  |  | нет |  |
| **Л4** | Основы информационной безопасности : учеб. пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - М. : Горячая линия-Телеком, 2006. | 10 |  |  |  |  | Ф(2)  ЧЗ1(2) |  |
| **Л5** | Правовое обеспечение информационной безопасности: учеб. пособие для вузов, 2-е издание. / Под ред. С.Я.Казанцева. М.: Издательский центр "Академия", 2007. | 10 |  | 10 |  |  | нет |  |

##### Дополнительная литература

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| **Д1** | Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. | нет |
| **Д2** | Серго А. Интернет и право. М., 2003. | СЭЛ(1) |
| **Д3** | Тедеев А.А. Информационное право: Учебник. – М.: Изд-во Эксмо, 2005. | нет |

|  |  |
| --- | --- |
| Зав. отделом учебной литературы *(для технических дисциплин)* | Киселева Т.В |

|  |  |
| --- | --- |
| Автор: |  |
| д.п.н., профессор  к.т.н., профессор | Чернолес В.П.  Шехунова Н.А. |
|  |  |
| Рецензент |  |
| к.т.н., доцент | Павлов С.М. |
|  |  |
| Зав. кафедрой автоматизированных систем обработки информации управленияи и управления |  |
| д.т.н., профессор | Советов Б.Я. |
|  |  |
| Декан факультета компьютерных технологий и информатики |  |
| д.т.н., профессор | Куприянов М.С. |
|  |  |
| Программа согласована: |  |
|  |  |
| Председатель методической комиссии факультета *компьютерных*  *технологий и информатики* |  |
| к.т.н., доц. | Михалков В.А. |
|  |  |
| Руководитель методического отдела |  |
| к.т.н., доцент | Марасина Л.А. |
|  |  |