Учреждение образования

«Белорусский государственный университет

информатики и радиоэлектроники»

УТВЕРЖДАЮ

Проректор по учебной работе

и менеджменту качества

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.Н. Живицкая

"25"ноября 2015 г.

Регистрационный № УД-6-307/р.

**«Основы защиты информации»**

Учебная программа учреждения высшего образования по учебной дисциплине для:

направлений образования

28 Электронная экономика, 39 Радиоэлектронная техника,

40 Информатика и вычислительная техника,

41 Компоненты оборудования, 45 Связь;

группы специальностей 36 04 Радиоэлектроника;

специальностей

1-53 01 02 Автоматизированные системы обработки информации,

1-53 01 07 Информационные технологии и управление

в технических системах,

1-58 01 01 Инженерно-психологическое обеспечение

информационных технологий,

1-98 01 02 Защита информации в телекоммуникациях

#### Кафедра защиты информации

|  |  |
| --- | --- |
| Всего часов по |  |
| дисциплине 94 |  |
| Зачетных единиц 2,5 |  |

2015 г.

Учебная программа учреждения высшего образования составлена на основе типовой учебной программы “Основы защиты информации”, утвержденной Министерством образования Республики Беларусь “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г., регистрационный номер №  ТД – /тип. и учебных планов специальностей по направлениям 28, 39, 40, 41, 45; группы специальностей 36 04; специальностей 1-53 01 02, 1-53 01 07, 1-58 01 01, 1-98 01 02.

Составитель:

Н.В.Насонова, доцент кафедры защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент

Рассмотрена и рекомендована к утверждению:

Кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники (протокол № 16 от 22.04.2015);

Научно-методическим советомучреждения образования «Белорусский государственный университет информатики и радиоэлектроники (протокол № 2 от 20.11.2015)

СОГЛАСОВАНО

Эксперт-нормоконтролер

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**План учебной дисциплины в дневной форме обучения:**

| Код специальности | Название специальности | Курс | Семестр | Аудиторных часов | | | | Академ. часов на курс. работу (проект) | Форма текущей аттестации |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Всего | Лекции | Лабораторные  занятия | Практические занятия ,семинары |
| **Факультет компьютерного проектирования** | | | | | | | | | |
| 1-36 04 01 | Программно-управляемые электронно-оптические системы | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-39 02 01 | Моделирование и компьютерное проектирование радиоэлектронных средств | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-39 02 02 | Проектирование и производство программно-управляемых электронных средств | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-39 02 03 | Медицинская электроника | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-39 03 01 | Электронные системы безопасности | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-39 03 02 | Программируемые мобильные системы | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-58 01 01 | Инженерно-психологическое обеспечение информационных технологий | 2 | 4 | 52 | 34 |  | 18 | - | зачет |
| 1-40 05 01-09 | Информационные системы и технологии (в обеспечении промышленной безопасности) | 2 | 4 | 52 | 34 |  | 18 | - | зачет |
| 1-40 05 01-10 | Информационные системы и технологии (в бизнес-менеджменте) | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| **Факультет информационных технологий и управления** | | | | | | | | | |
| 1-40 03 01 | Искусственный интеллект | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-36 04 02 | Промышленная электроника | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-53 01 02 | Автоматизированные системы обработки информации | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-53 01 07 | Информационные технологии и управление в технических системах | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| **Военный факультет** | | | | | | | | | |
| 1-39 01 01-03 | Радиотехника (специальные системы радиолокации и радионавигации) | 2 | 3 | 52 | 34 | - | 18 | - | зачет |
| 1-45 01 01-03 | Инфокоммуникационные технологии (системы телекоммуникаций специального назначения) | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| **Факультет радиотехники и электроники** | | | | | | | | | |
| 1-39 01 01-01 | Радиотехника (программируемые радиоэлектронные средства) | 2 | 3 | 52 | 34 | - | 18 | - | зачет |
| 1-39 01 01-02 | Радиотехника (техника цифровой радиосвязи) | 2 | 3 | 52 | 34 | - | 18 | - | зачет |
| 1-39 01 02 | Радиоэлектронные системы | 2 | 3 | 52 | 34 | - | 18 | - | зачет |
| 1-39 01 03 | Радиоинформатика | 2 | 3 | 52 | 34 | - | 18 | - | зачет |
| 1-39 01 04 | Радиоэлектронная защита информации | 2 | 3 | 52 | 34 | - | 18 | - | зачет |
| 1-39 03 03 | Электронные и информационно-управляющие системы физических установок | 2 | 3 | 52 | 34 | - | 18 | - | зачет |
| I-41 01 02 | Микро- и наноэлектронные технологии и системы | 2 | 3 | 52 | 34 | - | 18 | - | зачет |
| I-41 01 03 | Квантовые информационные системы | 2 | 3 | 52 | 34 | - | 18 | - | зачет |
| 1-41 01 04 | Нанотехнологии и наноматериалы в электронике | 2 | 3 | 52 | 34 | - | 18 | - | зачет |
| **Факультет компьютерных систем и сетей** | | | | | | | | | |
| 1-40 01 01 | Программное обеспечение информационных технологий | 3 | 5 | 52 | 34 | - | 18 | - | зачет |
| 1-40 02 02 | Электронные вычислительные средства | 3 | 5 | 52 | 34 | - | 18 | - | зачет |
| I-40 02 01 | Вычислительные машины, системы и сети | 3 | 5 | 52 | 34 | - | 18 | - | зачет |
| 1-40 04 01 | Информатики и технологии программирования | 3 | 5 | 52 | 34 | - | 18 | - | зачет |
| **Факультет телекоммуникаций** | | | | | | | | | |
| 1-45 01 01-01 | Инфокоммуникационные технологии (системы телекоммуникаций) | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-45 01 01-02 | Инфокоммуникационные технологии (сети инфокоммуникаций) | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-45 01 01-04 | Инфокоммуникационные технологии (цифровое теле- и радиовещание) | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-45 01 01-05 | Инфокоммуникационные технологии (системы распределения мультимедийной информации) | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-45 01 01-06 | Инфокоммуникационные технологии (лазерные информационно-измерительные системы) | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-45 01 02-01 | Инфокоммуникационные системы (стандартизация, сертификация и контроль параметров) | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-98 01 02 | Защита информации в телекоммуникациях | 2 | 3 | 52 | 34 | - | 18 | - | зачет |
| **Инженерно-экономический факультет** | | | | | | | | | |
| 1-28 01 02 | Электронный маркетинг | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-28 01 01 | Экономика электронного бизнеса | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-40 05 01-02 | Информационные системы и технологии (в экономике) | 2 | 4 | 52 | 34 | - | 18 | - | зачет |
| 1-40 05 01-08 | Информационные системы и технологии (в логистике) | 2 | 4 | 52 | 34 | - | 18 | - | зачет |

**План учебной дисциплины в вечерней форме обучения:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код специальности | Название специальности | Курс | Семестр | Аудиторных часов | | | | Академ. часов на курс. работу (проект) | Форма текущей аттестации |
| Всего | Лекции | Лабораторные  занятия | Практические занятия ,семинары |
| 1-53 01 07 | Информационные технологии и управление в технических системах | 3 | 6 | 34 | 16 | - | 18 | - | зачет |
| 1-40 02 01 | Вычислительные машины, системы и сети | 3 | 6 | 34 | 16 | - | 18 | - | зачет |

**План учебной дисциплины в заочной форме обучения:**

| Код специальности | Название специальности | Курс | Семестр | Аудиторных часов | | | | Академ. часов на курс. работу (проект) | Контрольныеработы | Форма текущей аттестации |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Всего | Лекции | Лабораторные  занятия | Практические занятия ,семинары |
| 1-39 02 02 | Проектирование и производство программно-управляемых электронных средств | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-39 02 01 | Моделирование и компьютерное проектирование радиоэлектронных средств | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-39 03 01 | Электронные системы безопасности | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-39 02 03 | Медицинская электроника | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-53 01 07 | Информационные технологии и управление в технических системах | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-41 01 02 | Микро- и наноэлектронные технологии и системы | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-39 01 01-01 | Радиотехника (программируемые радиоэлектронные средства) | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-40 02 01 | Вычислительные машины, системы и сети | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-45 01 01-02 | Инфокоммуникационные технологии (сети инфокоммуникаций) | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-45 01 01-01 | Инфокоммуникационные технологии (системы телекоммуникаций) | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-45 01 01-04 | Инфокоммуникационные технологии (цифровое теле- и радиовещание) | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-28 01 01 | Экономика электронного бизнеса | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-40 05 01-02 | Информационные системы и технологии (в экономике) | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-40 02 02 | Электронные вычислительные средства | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |
| 1-58 01 01 | Инженерно-психологическое обеспечение информационных технологий | 3 | 6 | 12 | 8 | - | 4 | - | 1 | зачет |

**План учебной дисциплины в дистанционной форме обучения:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код специальности | Название специальности | Курс | Семестр | Всего | Количество работ | | | Академ. часов на курс. работа (проект) | Форма текущей аттестации |
| Контрольные работы | Лабораторные  занятия | Индивидуальная практическая работа |
| 1-58 01 01 | Инженерно-психологическое обеспечение информационных технологий | 3 | 6 | 94 | 2 | - | - | - | зачет |
| 1-40 05 01-02 | Информационные системы и технологии (в экономике) | 3 | 6 | 94 | 2 | - | - | - | зачет |
| 1-53 01 02 | Автоматизированные системы обработки информации | 5 | 10 | 94 | 2 | - | - | - | зачет |
| 1-40 03 01 | Искусственный интеллект | 5 | 9 | 94 | 2 | - | - | - | зачет |
| 1-40 04 01 | Информатика и технологии программирования | 4 | 7 | 94 | 2 | - | - | - | зачет |
| 1-40 01 01 | Программное обеспечение информационных технологий | 5 | 9 | 94 | 2 | - | - | - | зачет |
| 1-28 01 02 | Электронный маркетинг | 2 | 3 | 94 | 2 | - | - | - | зачет |
| 1-40 05 01-10 | Информационные системы и технологии (в бизнес-менеджменте) | 3 | 6 | 94 | 2 |  | - | - | зачет |
| 1-28 01 01 | Экономика электронного бизнеса | 2 | 3 | 94 | 2 |  | - | - | зачет |
| 1-39 03 02 | Программируемые мобильные системы | 3 | 6 | 94 | 2 |  | - | - | зачет |

**План учебной дисциплины в дневной форме обучения**

**для получения высшего образования,**

**интегрированного со средним специальным образованием:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код специальности | Название специальности | Курс | Семестр | Аудиторных часов | | | | Академ. часов на курс. работу (проект) | Форма текущей аттестации |
| Всего | Лекции | Лабораторные  занятия | Практические занятия ,семинары |
| 1-39 03 03 | Электронные и информационно-управляющие системы физических установок | 1 | 1 | 52 | 34 | - | 18 | - | зачет |
| 1-41 01 02 | Микро- и наноэлектронные технологии и системы | 1 | 1 | 52 | 34 | - | 18 | - | зачет |

**План учебной дисциплины в вечерней форме обучения**

**для получения высшего образования,**

**интегрированного со средним специальным образованием:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код специальности | Название специальности | Курс | Семестр | Аудиторных часов | | | | Академ. часов на курс. работу (проект) | Форма текущей аттестации |
| Всего | Лекции | Лабораторные  занятия | Практические занятия ,семинары |
| 1-40 02 01 | Вычислительные машины, системы и сети | 2 | 4 | 18 | 10 | -- | 8 |  | зачет |
| 1-40 01 01 | Программное обеспечение информационных технологий | 3 | 5 | 18 | 10 | -- | 8 |  | зачет |
| 1-53 01 07 | Информационные технологии и управление в технических системах | 2 | 4 | 18 | 10 | -- | 8 |  | зачет |
| 1-58 01 01 | Инженерно-психологическое обеспечение информационных технологий | 3 | 5 | 18 | 10 | -- | 8 |  | зачет |

**План учебной дисциплины в заочной форме обучения для получения высшего образования, интегрированного со средним специальным**

**образованием:**

| Код специальности | Название специальности | Курс | Семестр | Аудиторных часов | | | | Академ. часов на курс. работу (проект) | Контрольные работы | Форма текущей аттестации |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Всего | Лекции | Лабораторные  занятия | Практические занятия ,семинары |
| 1-40 01 01 | Программное обеспечение информационных технологий | 2 | 3 | 8 | 4 | - | 4 | - | 1 | зачет |
| 1-28 01 01 | Экономика электронного бизнеса | 2 | 3 | 8 | 4 | - | 4 | - | 1 | зачет |
| 1-40 05 01-02 | Информационные системы и технологии (в экономике) | 2 | 3 | 8 | 4 | - | 4 | - | 1 | зачет |
| 1-53 01 07 | Информационные технологии и управление в технических системах | 2 | 3 | 8 | 4 | - | 4 | - | 1 | зачет |
| 1-45 01 01-04 | Инфокоммуникационные технологии (цифровое теле–и радиовещание) | 2 | 3 | 8 | 4 | - | 4 | - | 1 | зачет |
| 1-36 04 02 | Промышленная электроника | 2 | 3 | 8 | 4 | - | 4 | - | 1 | зачет |
| 1-39 03 01 | Электронные системы безопасности | 2 | 3 | 8 | 4 | - | 4 | - | 1 | зачет |
| 1-58 01 01 | Инженерно-психологическое обеспечение информационных технологий | 2 | 3 | 8 | 4 | - | 4 | - | 1 | зачет |
| 1-39 03 02 | Программируемые мобильные системы | 2 | 3 | 8 | 4 | - | 4 | - | 1 | зачет |

**Место дисциплины.**

Интенсивное внедрение информационных технологий во все области деятельности человека позволяет обеспечить оперативный обмен сведениями между службами, отделами предприятия и организациями в целом за счет оптимизации информационных потоков, что позволяет ускорить и сделать более качественным процесс их взаимодействия. Сведения, которыми обмениваются такие партнеры, как правило, носят конфиденциальный характер и относятся к категориям служебной или государственной тайны, что требует подготовки современных специалистов, обладающих не только специальными знаниями по их профилю обучения, но и владением основами защиты информации.

Цель учебной дисциплины: получение базовых знаний по вопросам обеспечения защиты информации в условиях различных по виду, происхождению и характеру возникновения угроз.

Задачи учебной дисциплины:

– изучение угроз информационной безопасности;

– изучение методов и средств защиты информации;

– получение знаний о принципах организации и построения комплексных систем защиты информации.

В результате изучения учебной дисциплины «Основы защиты информации» формируются следующие:

**академические:**

1. умение применять базовые научно-теоретические знания для решения теоретических и практических задач;
2. владение системным и сравнительным анализом;
3. владение исследовательскими навыками;
4. умение работать самостоятельно;
5. способность порождать новые идеи (обладание креативностью);
6. владение междисциплинарным подходом при решении проблем
7. обладание навыками, связанными с использованием технических устройств, управлением информацией и работой с компьютером;
8. обладание навыками устной и письменной коммуникации;
9. умение учиться, повышать свою квалификацию в течение всей жизни;
10. способность использовать основные законы естественнонаучных дисциплин в профессиональной деятельности;
11. владение основными методами, способами и средствами получения, хранения, переработки информации с использованием компьютерной техники;
12. умение на научной основе организовывать свой труд, самостоятельно оценивать результаты своей деятельности;

социально-личностные:

1. обладание качествами гражданственности;
2. способность к социальному взаимодействию;
3. обладание способностью к межличностным коммуникациям;
4. способность к критике и самокритике;
5. умение работать в команде

**профессиональные:**

1. умение проводить предпроектное обследование, выявлять информационные потребности заказчика и формировать требования к автоматизированной информационной системе в сфере электронного бизнеса;
2. умение работать с юридической литературой и трудовым законодательством;
3. умение пользоваться глобальными информационными ресурсами;
4. владение современными средствами инфокоммуникаций;
5. умение формулировать цели и ставить задачи проектирования;
6. способность осуществлять сбор, анализ и изучение научно-технической информации, отечественного и зарубежного опыта по тематике проекта;
7. способность разрабатывать план и техническое задание на проектирование или модернизацию радиоэлектронных устройств и систем, информационных систем;
8. умение проводить проектные расчеты и технико-экономическое обоснование принимаемых решений;
9. умение разрабатывать модели объектов и процессов с целью анализа и оптимизации их параметров с использованием имеющихся средств исследований, включая стандартные пакеты прикладных программ;
10. умение разрабатывать структурные, функциональные схемы радиоэлектронных систем и сетей передачи данных, принципиальные схемы устройств с использованием средств компьютерного проектирования;
11. умение проводить испытание аппаратных и программных средств радиоэлектронных устройств и систем, сетей передачи данных;
12. умение разрабатывать проектную и рабочую техническую документацию, оформление законченных проектно-конструкторских работ;
13. способность контролировать соответствие разрабатываемых проектов и технической документации техническим регламентам, национальным стандартам, техническим условиям и другим нормативным документам;
14. умение оценивать конкурентоспособность и экономическую эффективность разрабатываемых технологий;
15. умение проводить опытно-технологические работы при освоении новых технологий, опытно-промышленную проверку и испытания разрабатываемых изделий;
16. умение разрабатывать бизнес-планы создания новых радиотехнических устройств, в том числе и систем;
17. способность анализировать состояние научно-технической проблемы на основе подбора и изучения литературных и патентных источников;
18. умение составлять обзоры и отчеты по результатам проводимых исследований;
19. способность учитывать результаты научно-исследовательских и опытно-конструкторских работ в процессе разработки технических заданий на проектируемые радиоэлектронные и информационные системы;
20. умение взаимодействовать со специалистами смежных профилей;
21. владение основами патентной и лицензионной деятельности;
22. умение анализировать и оценивать собранные данные;
23. умение вести переговоры с другими заинтересованными участниками;
24. способность готовить доклады, статьи и материалы к презентациям;
25. умение представлять результаты исследования в формах отчетов, рефератов публикаций, презентаций и публичных обсуждений, формулировать практические рекомендации по использованию результатов научных исследований;
26. умение готовить проекты лицензионных договоров о передаче прав на использование объектов интеллектуальной собственности.
27. способность организовывать и проводить патентные исследования и библиографический поиск в области защиты информации и телекоммуникаций.

В результате изучения учебной дисциплины обучаемый должен:

***знать:***

* системную методологию и правовое обеспечение защиты информации;
* организационно-технические методы и технические средства защиты информации;
* основы криптографической защиты информации;
* особенности защиты информации в автоматизированных системах;
* основные положения международного и национального законодательства в области интеллектуальной собственности;
* порядок оформления и защиты прав на объекты интеллектуальной собственности;

***уметь:***

* определять возможные каналы утечки информации и обоснованно выбирать средства их блокирования;
* разрабатывать рекомендации по защите объектов различного типа от несанкционированного доступа;
* проводить патентные исследования;
* составлять заявки на выдачу охранных документов на объекты промышленной собственности;
* оформлять договора на передачу имущественных прав на объекты интеллектуальной собственности;

***владеть:***

* основными приемами анализа вероятных угроз информационной безопасности для заданных объектов;
* способами введения объектов интеллектуальной собственности в гражданский оборот;
* способами передачи прав на использование объектов интеллектуальной собственности.

**Перечень дисциплин,**

**усвоение которых необходимо для изучения курса:**

|  |  |  |
| --- | --- | --- |
| **№ пп** | **Название дисциплины** | **Раздел, тема** |
| 1. | Физика | Тема 1.9. Волновые процессы  Раздел 3. Электричество и магнетизм  Раздел 4. Оптика |
| 2. | Математика | Весь курс |

**1.Содержание учебной дисциплины**

| №  тем | Наименование  разделов, тем | Содержание тем |
| --- | --- | --- |
|  | Раздел 1. Методология информационной безопасности | |
| 1 | Основные понятия и определения в сфере защиты информации. Охраняемые сведения и их демаскирующие признаки. Классификация угроз ИБ и методов ЗИ | Задачи в сфере обеспечения информационной безопасности. Информация общего и ограниченного распространения. Угрозы информационной безопасности. Классификация угроз безопасности по виду, происхождению, источникам и характеру возникновения. Обеспечение доступности, конфиденциальности и целостности информации. Защита информации от случайных видов угроз. |
|  | Раздел 2. Правовые и организационные методы защиты информации | |
| 2 | Государственное регулирование в сфере защиты информации | Информационные технологии и право. Основные законы РБ в области компьютерного права. Правовая защита от компьютерных преступлений. Государственное регулирование в области защиты информации. Международные стандарты и рекомендации в области ИБ. |
| 3 | Нормативно-правовое обеспечение защиты информации в организации. Коммерческая тайна. Политика ИБ. | Основные принципы создания системы менеджмента информационной безопасности. Анализ рисков. Отнесение сведений к коммерческой тайне и их защита. Назначение и цель политики ИБ. |
| 4 | Организационные меры по защите информации | Защита информационных активов организации. Защита человеческих ресурсов перед наймом, во время и по окончании работы. Организация безопасных зон и защита оборудования. Процедуры эксплуатации и рабочие обязанности. Резервное копирование. Обращение с носителями информации и правила по обмену информацией. Постоянный контроль. Обязанности пользователей. |
| 5 | Социальный инжиниринг | Основные принципы воздействия. Техники социнжиниринга. Методы противодействия. |
|  | Раздел 3. Защита информации от утечки по техническим каналам | |
| 6 | Классификация технических каналов утечки информации по физическим принципам возникновения | Классификация каналов утечки информации. Особенности технических каналов утечки информации. Акустический канал утечки информации. Электромагнитный канал утечки информации. Источники образования технических каналов утечки информации. |
| 7 | Защита речевой информации. Защита информации от утечки за счет побочных электромагнитных излучений и наводок. Выявление закладных устройств | Технические методы защиты информации. Организация защищенных помещений. Пассивные методы защиты информации: звукоизоляция, фильтрация, экранирование. Активные методы защиты информации: акустическая маскировка речи, электромагнитное зашумление, защита проводных линий. Технические средства защиты. Виды технических средств несанкционированного доступа. Классификация поисковых работ по выявлению закладных устройств. Метод нелинейной локации. Методы и технические средства выявления сигналов подслушивающих устройств. |
|  | Раздел 4. Инженерно-техническая защита объектов от несанкционированного доступа | |
| 8 | Техническая укрепленность периметра защищаемого объекта. Системы охранно-пожарной сигнализации | Интегральная система безопасности. Системы механической защиты. Системы обнаружения. Виды датчиков. Средства пожарной сигнализации. |
| 9 | Системы видеонаблюдения. Системы контроля и управления доступом | Системы видеонаблюдения. Состав системы контроля и управления доступом. Идентификация и аутентификация, основные технологии. |
|  | Раздел 5. Защита информации в информационных системах | |
| 10 | Вредоносные программы и антивредоносное ПО. Управление логическим доступом | Методы программной защиты информации. Классификация вредоносных программ. Защита от компьютерных вирусов и шпионажного ПО. Дискреционный метод организации разграничения доступа. Мандатный метод организации разграничения доступа. |
| 11 | Основы построения криптосистем | Классификация методов шифрования. Алгоритмы шифрования. Ключевая информация. Криптографические протоколы. Хэш-функции. Протокол электронной подписи RSA. Электронно‑цифровая подпись. Инфраструктура открытых ключей. Контроль целостности информации. |
| 12 | Обеспечение безопасности в системах электронной коммерции | Идентификация, аутентификация и авторизация. Технологии аутентфикации. Сервер аутентификации Kerberos. Общая схема электронных платежных систем. Платежные средства. Обеспечение безопасности электронных платежей через сеть Internet: протоколы SSL (Secure Sockets Layer), SET (Secure Electronic Transaction). Защита информации, хранящейся на рабочих станциях. |
| 13 | Противодействие атакам | Основы сетевой безопасности. Атаки в компьютерных сетях. Сетевые сервисы безопасности. Межсетевые экраны. Системы обнаружения вторжений. Виртуальные частные сети. |
|  | Раздел 6. Основы управления интеллектуальной собственностью | |
| 14 | Авторское право и смежные права | Понятие интеллектуальной собственности. Объекты авторского права и смежных прав. Ограничения имущественных прав. Срок действия авторского права. Принципы и условия возникновения, реализации и защиты авторских и смежных прав. Управление имущественными правами авторов и обладателей смежных прав на коллективной основе. Авторский договор. |
| 15 | Промышленная собственность | Объекты промышленной собственности. Субъекты права промышленной собственности. Система выдачи охранных документов. Условия патентоспособности объектов промышленной собственности |
| 16 | Патентные исследования | Патентная информация, ее видовой состав и особенности. Исследование технического уровня и тенденций развития объектов техники, их патентоспособности, патентной чистоты, конкурентоспособности. Особенности проведения патентных исследований на стадиях и этапах жизненного цикла продукции. |
| 17 | Коммерческое использование объектов интеллектуальной собственности. Защита прав авторов и правообладателей | Основные формы передачи прав на объекты интеллектуальной собственности. Классификация договоров их структура и содержание. Лицензионный договор. Виды лицензий. Организация работ по продаже лицензий. Договор уступки. Государственная регистрация договоров. Защита прав авторов и правообладателей |

**2. ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ**

**2.1 Литература**

**2.1.1 Основная**

1. Лыньков, Л. М. Основы защиты информации и управление интеллектуальной собственностью : учеб.-метод. пособие / Л. М. Лыньков, В. Ф. Голиков, Т. В. Борботько. – Минск : БГУИР, 2013.
2. Бузов, Г. А. Защита от утечки информации по техническим каналам : учеб. пособие для подготовки экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия – Телеком, 2005.
3. Торокин, А. А. Инженерно-техническая защита информации / А. А. Торокин. – М. : Гелиос АРВ, 2005.
4. Магауенов, Р. Г. Системы охранной сигнализации: основы теории и принципы построения : учеб. пособие / Р. Г. Магауенов. – М. : Горячая линия – Телеком, 2004.
5. Синилов, В. Г. Системы охранной, пожарной и охранно-пожарной сигнализации / В. Г. Синилов. – М. : Академия, 2010.
6. Дамьяновски, В. CCTV. Библия видеонаблюдения. Цифровые и сетевые технологии / В. Дамьяновски. – М. : ООО “Ай-Эс-Эс Пресс”, 2006.
7. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – М. : ДМК, 2000.
8. Кудашов, В. И. Интеллектуальная собственность: охрана и реализация прав, управление: учеб. пособие / В. И. Кудашов. – Минск : БНТУ, 2004.
9. Волынец-Руссет, Э. Я. Коммерческая реализация изобретений и ноу-хау (на внешних и внутренних рынках): учебник / Э. Я. Волынец-Руссет. – М. : Экономист, 2004.
10. Якимахо, А. П. Управление объектами интеллектуальной собственности в Республике Беларусь / А. П. Якимахо. – Минск : Амалфея, 2005.

**2.1.2 Дополнительная**

1. Ворона, В.А. Технические средства наблюдения в охране объектов / В. А. Ворона, В. А. Тихонов. – М. : Горячая линия – Телеком, 2011.
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В. Ф. Шаньгин. – М. : Издат. дом «Форум»: Инфра-М, 2011.
3. Деднев, М. А. Защита информации в банковском деле и электронном бизнесе / М.А. Деднев, Д.В. Дыльнов, М.А. Иванов. М. : Кудиц-образ, 2004.
4. Кудашов, В. И. Методическое пособие по вопросам введения в гражданский оборот результатов интеллектуальной деятельности / В. И. Кудашов, Т. И. Турлюк. Минск : РУП «РУПИС», 2004.

**2.2 Перечень компьютерных программ, наглядных и других пособий,**

**методических указаний и материалов, технических** **средств обучения**

1. Богуш В.А. Программа “Locator”. Минск, БГУИР, 2004 г.
2. Устройство защиты речевой информации «Прибой».
3. Программа «ГОСТ 28147-89».
4. [Голиков, В. Ф. Криптографическая защита информации в телекоммуникационных системах : учебно-метод. пособие : в 2 ч. Ч. 1 / В. Ф. Голиков, А. В. Курилович. – Минск : БГУИР, 2006.](http://172.16.33.2/Met/%D0%A4%D0%B0%D0%BA%D1%83%D0%BB%D1%8C%D1%82%D0%B5%D1%82%20%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B9%20%28%D0%A4%D0%A2%D0%9A%29/%D0%9A%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B0%20%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8/%D0%93%D0%BE%D0%BB%D0%B8%D0%BA%D0%BE%D0%B2,%20%D0%92.%20%D0%A4.%20%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC_%D0%B2_%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%D1%85_%D0%A7_1_.pdf)
5. [Основы защиты информации и управления интеллектуальной собственностью. Практикум : учебно-метод. пособие / Л. М. Лыньков [и др.]. – Минск : БГУИР, 2011.](http://172.16.33.2/Met/%D0%A4%D0%B0%D0%BA%D1%83%D0%BB%D1%8C%D1%82%D0%B5%D1%82%20%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B9%20%28%D0%A4%D0%A2%D0%9A%29/%D0%9A%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B0%20%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D1%8B_%D0%B7%D0%B0%D1%89_%D0%B8%D0%BD%D1%84_%D0%B8_%D1%83%D0%BF%D1%80_%D0%B8%D0%BD%D1%82%D0%B5%D0%BB_%D1%81%D0%BE%D0%B1%D1%81%D1%82%D0%B2_%D0%9F%D1%80%D0%B0%D0%BA%D1%82%D0%B8%D0%BA%D1%83%D0%BC_%D0%A3%D1%87_%D0%BC%D0%B5%D1%82_%D0%BF%D0%BE%D1%81.pdf)

**2.3. Перечень тем практических занятий, их название**

Целью практических занятий является закрепление теоретического курса, приобретение навыков решения задач, активизация самостоятельной работы студентов.

| № темы по п.1 | Название практического занятия | Содержание | Обеспеченность  по пункту 2.2 |
| --- | --- | --- | --- |
| 1, 3 | Описание информационного объекта. Классификация информации. | Изучение типового алгоритма описания информационной системы. Описание и классификация информационных ресурсов. | 5 |
| 3, 4, 5 | Анализ рисков информационной безопасности. | Изучение методик оценки необходимости защиты информационной системы и определения ожидаемых затрат на защиту информации. | 5 |
| 6 | Оценка эффективности защиты речевой информации | Изучение методики специальных исследований при защите речевой информации | 5 |
| 7 | Акустическая маскировка речи. | Изучение активного метода защиты информации от утечки по акустическим каналам, ознакомление с устройством защиты речевой информации. | 1 |
| 7 | Защита информации от утечки через ПЭМИН пассивным методом. | Изучение пассивного метода защиты информации от утечки по электромагнитным каналам. Расчет параметров экрана электромагнитного излучения. | 2 |
| 7, 8, 9 | Организация выделенных помещений. | Изучение порядка организации выделенных помещений. Ознакомление с порядком и средствами проведения поисковых работ на обнаружение закладных устройств. | 5 |
| 11 | Алгоритм шифрования данных ГОСТ 28147-89. Режим простой замены. | Изучение симметричного алгоритма шифрования данных. | 5 |
| 14 | Составление и оформление авторского договора | Получение практических навыков составления и оформления авторского договора | 4 |
| 15, 16 | Составление и оформление заявок на объекты промышленной собственности | Исследование структуры и состава патентных документов. Составление и оформление заявок на объекты промышленной собственности | 3 |

**2.4. Контрольная работа, ее характеристика**

Студентами заочной формы обучения по обязательному модулю выполняется одна контрольная работа на основе индивидуальных заданий. Студентами дистанционной формы обучения по обязательному модулю выполняется две контрольных работы на основе индивидуальных заданий.

Материал контрольной работы необходимо излагать последовательно и аргументированно. Целью контрольной работы является углубление политологических знаний, приобретение исследовательских навыков.

| №  темы  по п.1 | Наименование варианта темы контрольной работы | Характеристика |
| --- | --- | --- |
| 1 | Угрозы информационной безопасности. Основные цели информационной безопасности | 1. Классификация угроз безопасности по виду, происхождению, источникам и характеру возникновения. Примеры 2. Обеспечение доступности, конфиденциальности и целостности информации. Защита информации от случайных видов угроз. |
| 2 | Информационные технологии и право. | 1. Основные законы РБ в области компьютерного права. 2. Государственное регулирование в области защиты информации. 3. Международные стандарты и рекомендации в области ИБ. |
| 3 | Система менеджмента информационной безопасности организации | 1. Основные принципы создания системы менеджмента информационной безопасности. 2. Анализ рисков. Этапы. |
| 3 | Коммерческая тайна и ее защита. | 1. Законодательные аспекты отнесения сведений к коммерческой тайне 2. Защиты информации, составляющей коммерческую тайну. |
| 4 | Политика информационной безопасности | 1. Назначение и цель политики ИБ 2. Содержание, структура, этапы разработки политики ИБ |
| 4 | Рекомендации по организации ИБ в организации. Защита активов. Защита человеческих ресурсов | 1. Защита информационных активов организации. 2. Защита человеческих ресурсов перед наймом, во время и по окончании работы. |
| 4 | Рекомендации по организации ИБ в организации. Физическая и экологическая безопасность. | 1. Организация безопасных зон и защита оборудования. 2. Процедуры эксплуатации и рабочие обязанности. 3. Резервное копирование. |
| 4 | Рекомендации по организации ИБ в организации. Обмен информацией. Постоянный контроль. Обязанности пользователей | 1. Обращение с носителями информации и правила по обмену информацией. 2. Постоянный контроль. 3. Обязанности пользователей. |
| 5 | Социнжиниринг | 1. Основные принципы воздействия. 2. Техники социнжиниринга. 3. Методы противодействия. |
| 6, 7 | Акустические каналы утечки информации | 1. Классификация акустических каналов утечки информации 2. Источники образования 3. Методы защиты от утечки |
| 6, 7 | Электромагнитные каналы утечки информации | 1. Классификация электромагнитных каналов утечки информации 2. Источники образования 3. Методы защиты от утечки |
| 6, 7, 8 | Технические методы и средства защиты информации | 1. Пассивные методы защиты информации: звукоизоляция, фильтрация, экранирование. 2. Активные методы защиты информации: акустическая маскировка речи, электромагнитное зашумление, защита проводных линий. 3. Технические средства защиты. |
| 7 | Технические средства разведки | 1. Виды технических средств несанкционированного доступа. 2. Классификация поисковых работ по выявлению закладных устройств. 3. Методы и технические средства выявления ТСР. |
| 8, 9 | Инженерно-техническая защита информации | 1. Системы механической защиты. 2. Системы обнаружения и видеонаблюдения. 3. Виды датчиков. 4. Состав системы контроля и управления доступом. 5. Интегральная система безопасности. |
| 10 | Защита от вредоносного ПО. | 1. Классификация вредоносных программ. 2. Средства защиты от компьютерных вирусов и шпионажного ПО. 3. Технологии работы антивредоносногоПО |
| 10 | Управление доступом | 1. Основные подходы к управлению доступом 2. Дискреционный метод организации разграничения доступа. 3. Мандатный метод организации разграничения доступа. 4. Ролевой метод разграничения доступом 5. Средства разграничения доступа |
| 11 | Контроль целостности информации. | 1. Назначение контроля целостности информации. 2. Основные технологии контроля целостности 3. Реализация контроля целостности в различных системах |
| 13 | Основы сетевой безопасности | 1. Атаки в компьютерных сетях. 2. Сетевые сервисы безопасности. 3. Межсетевые экраны. 4. Системы обнаружения вторжений. 5. Виртуальные частные сети. |
| 11 | Шифрование | 1. Классификация методов шифрования. 2. Алгоритмы шифрования. 3. Ключевая информация. 4. Криптографические протоколы. 5. Хэш-функции. |
| 11 | Электронная цифровая подпись | 1. Протокол электронной подписи RSA. 2. Принципы электронно‑цифровой подписи. 3. Применение ЭЦП (в т.ч. в Беларуси) |
| 11 | Инфраструктура открытых ключей | 1. Основные принципы организации инфраструктуры открытых ключей. Назначение 2. Основные компоненты ИОК 3. Применение ИОК |
| 12 | Идентификация, аутентификация и авторизация. | 1. Основные понятия. 2. Технологии аутентификации. 3. Сервер аутентификации Kerberos. |
| 12 | Электронные платежные системы | 1. Общая схема электронных платежных систем. 2. Виды платежных систем. 3. Платежные средства. 4. Обеспечение безопасности электронных платежей через сеть Internet: протоколы SSL (Secure Sockets Layer), SET (Secure Electronic Transaction). |
| 14 | Авторское право и смежные права | 1. Понятие интеллектуальной собственности. 2. Объекты и субъекты авторского права и смежных прав. 3. Ограничения имущественных прав. 4. Срок действия авторского права. |
| 14 | Защита авторских и смежных прав. Авторский договор | 1. Принципы и условия возникновения, реализации и защиты авторских и смежных прав. 2. Управление имущественными правами авторов и обладателей смежных прав на коллективной основе. 3. Авторский договор. |
| 15 | Право промышленной собственности | 1. Объекты промышленной собственности. 2. Субъекты права промышленной собственности. 3. Система выдачи охранных документов. 4. Международные договора в области права промышленной собственности |
| 16 | Объекты промышленной собственности. | 1. Условия патентоспособности объектов промышленной собственности. 2. Патентная информация, ее видовой состав и особенности. |
| 17 | Передача прав на объекты интеллектуальной собственности | 1. Основные формы передачи прав на объекты интеллектуальной собственности. 2. Классификация договоров их структура и содержание. 3. Лицензионный договор. Виды лицензий. 4. Договор уступки. |

\* Вариант задания контрольной работы для заочной формы обучения выдается студенту преподавателем из предложенных

\*\* Для студентов дистанционной формы обучения преподаватель задает два варианта для каждой контрольной работы из предложенных

**3.1 Учебно-методическая карта учебной дисциплины в дневной форме обучения в т.ч. в дневной форме обучения для получения высшего образования, интегрированного со средним специальным образованием**

| Номер раздела, темы по п.1 | Название раздела, темы | Количество аудиторных часов | | | Самостоятельная работа, часы | Форма контроля знаний студентов |
| --- | --- | --- | --- | --- | --- | --- |
| ЛК | ПЗ | Лаб. зан. |
| Раздел 1. Методология информационной безопасности | | **2** | **2** |  | **4** |  |
| 1 | Основные понятия и определения в сфере защиты информации. Охраняемые сведения и их демаскирующие признаки. Классификация угроз ИБ и методов ЗИ | 2 | 2 |  | 4 | тест-опрос |
| Раздел 2. Правовые и организационные методы защиты информации | | **8** | **2** |  | **8** |  |
| 2 | Государственное регулирование в сфере защиты информации | 2 |  |  | 2 | фронтальный опрос |
| 3 | Нормативно-правовое обеспечение защиты информации в организации. Коммерческая тайна. Политика ИБ. | 2 | 2 |  | 2 | тест-опрос |
| 4 | Организационные меры по защите информации | 2 |  |  | 2 | фронтальный опрос |
| 5 | Социальный инжиниринг | 2 |  |  | 2 | фронтальный опрос |
| Раздел 3. Защита информации от утечки по техническим каналам | | **4** | **6** |  | **8** |  |
| 6 | Классификация технических каналов утечки информации по физическим принципам возникновения | 2 | 2 |  | 4 | тест-опрос |
| 7 | Защита речевой информации. Защита информации от утечки за счет побочных электромагнитных излучений и наводок. Выявление закладных устройст. | 2 | 4 |  | 4 | тест-опрос |
| Раздел 4. Инженерно-техническая защита объектов от несанкционированного доступа | | **2** | **2** |  | **2** |  |
| 8 | Техническая укрепленность периметра защищаемого объекта. Системы охранно-пожарной сигнализации | 1 | 1 |  | 1 | тест-опрос |
| 9 | Системы видеонаблюдения. Системы контроля и управления доступом | 1 | 1 |  | 1 | тест-опрос |
| Раздел 5. Защита информации в информационных системах | | **10** | **2** |  | **12** |  |
| 10 | Вредоносные программы и антивредоносное ПО. Управление логическим доступом | 2 |  |  | 2 | фронтальный опрос |
| 11 | Основы построения криптосистем | 2 | 2 |  | 2 | тест-опрос |
| 12 | Обеспечение безопасности в системах электронной коммерции | 2 |  |  | 4 | фронтальный опрос |
| 13 | Противодействие атакам | 4 |  |  | 4 | фронтальный опрос |
| Раздел 6. Основы управления интеллектуальной собственностью | | **8** | **4** |  | **8** |  |
| 14 | Авторское право и смежные права | 2 | 2 |  | 2 | тест-опрос |
| 15 | Промышленная собственность | 2 |  |  | 2 | фронтальный опрос |
| 16 | Патентные исследования | 2 | 2 |  | 2 | тест-опрос |
| 17 | Коммерческое использование объектов интеллектуальной собственности. Защита прав авторов и правообладателей | 2 |  |  | 2 | фронтальный опрос |
|  | Текущая аттестация |  |  |  |  | зачет |
|  | Итого | **34** | **18** |  | **42** |  |

**3.2. Учебно-методическая карта учебной дисциплины в вечерней форме обучения**

| Номер раздела, темы по п.1 | Название раздела, темы | Количество аудиторных часов | | Самостоятельная работа, часы | Форма контроля знаний студентов |
| --- | --- | --- | --- | --- | --- |
| ЛК | ПЗ |
| Раздел 1. Методология информационной безопасности | | | | | |
| 1 | Введение. Основные понятия ИБ. Основные виды защищаемых сведений. Классификация угроз | 1 | 2 | 2 | Тестирование, оценка рефератов |
| Раздел 2. Правовые и организационные методы защиты информации | | | | | |
| 2 | Государственное регулирование в сфере защиты информации | 1 |  | 4 | Устный опрос |
| 3 | Нормативно-правовое обеспечение защиты информации в организации. Коммерческая тайна. Политика ИБ. | 1 | 2 | 4 | Тестирование, оценка рефератов |
| 4 | Организационные меры по защите информации | 2 |  | 4 | Устный опрос |
| 5 | Социальный инжиниринг | 1 |  | 4 | Устный опрос |
| Раздел 3. Защита информации от утечки по техническим каналам | | | | | |
| 6 | Классификация технических каналов утечки информации по физическим принципам возникновения | 0,5 | 2 | 2 | Тестирование, оценка рефератов |
| 7 | Защита речевой информации. Защита информации от утечки за счет побочных электромагнитных излучений и наводок. Выявление закладных устройств | 1 | 4 | 4 | Тестирование, оценка рефератов |
| Раздел 4. Инженерно-техническая защита объектов от несанкционированного доступа | | | | | |
| 8 | Техническая укрепленность периметра защищаемого объекта. Системы охранно-пожарной сигнализации | 0,5 | 1 | 2 | Тестирование, оценка рефератов |
| 9 | Системы видеонаблюдения. Системы контроля и управления доступом | 0,5 | 1 | 2 | Тестирование, оценка рефератов |
| Раздел 5. Защита информации в информационных системах | | | | | |
| 9 | Вредоносные программы и антивредоносное ПО. Управление логическим доступом | 0,5 |  | 4 | Устный опрос |
| 11 | Основы построения криптосистем | 1 | 2 | 4 | Тестирование, оценка рефератов |
| 12 | Обеспечение безопасности в системах электронной коммерции | 1 |  | 4 | Устный опрос |
| 10 | Основы сетевой безопасности. | 1 |  | 4 | Устный опрос |
| Раздел 6. Основы управления интеллектуальной собственностью | | | | | |
| 13 | Авторское право и смежные права | 1 | 2 | 4 | Тестирование, оценка рефератов |
| 14 | Промышленная собственность | 1 |  | 4 | Устный опрос |
| 15 | Патентные исследования | 1 | 2 | 4 | Тестирование, оценка рефератов |
| 16 | Коммерческое использование объектов интеллектуальной собственности. Защита прав авторов и правообладателей | 1 |  | 4 | Устный опрос |
|  | Текущая аттестация |  |  |  | зачет |
|  | Итого | 16 | 18 | 60 |  |

**3.3. Учебно-методическая карта учебной дисциплины в заочной форме обучения**

| Номер раздела, темы по п.1 | Название раздела, темы | Количество аудиторных часов | | Самостоятельная работа, часы | Форма контроля знаний студентов |
| --- | --- | --- | --- | --- | --- |
| ЛК | ПЗ |
| Раздел 1. Методология информационной безопасности | | | | | |
| 1 | Основные понятия и определения в сфере защиты информации. Охраняемые сведения и их демаскирующие признаки. Классификация угроз ИБ и методов ЗИ | 1 |  | 4 | Устный опрос, защита КР соответствующего варианта |
| Раздел 2. Организационные методы защиты информации | | | | | |
| 2 | Государственное регулирование в сфере защиты информации | - |  | 4 | Устный опрос, защита КР соответствующего варианта |
| 3 | Нормативно-правовое обеспечение защиты информации в организации. Коммерческая тайна. Политика ИБ. | 1 | 2 | 4 | Тестирование, защита КР |
| 4 | Организационные меры по защите информации | - |  | 8 | Устный опрос, защита КР соответствующего варианта |
| 5 | Социальный инжиниринг | - |  | 6 | Устный опрос, защита КР соответствующего варианта |
| Раздел 3. Защита информации от утечки по техническим каналам | | | | | |
| 6 | Классификация технических каналов утечки информации по физическим принципам возникновения | - |  | 4 | Устный опрос, защита КР соответствующего варианта |
| 7 | Защита речевой информации. Защита информации от утечки за счет побочных электромагнитных излучений и наводок. Выявление закладных устройств | 2 |  | 6 | Устный опрос, защита КР соответствующего варианта |
| Раздел 4. Инженерно-техническая защита объектов от несанкционированного доступа | | | | | |
| 8 | Техническая укрепленность периметра защищаемого объекта. Системы охранно-пожарной сигнализации | 0,5 |  | 2 | Устный опрос, защита КР соответствующего варианта |
| 9 | Системы видеонаблюдения. Системы контроля и управления доступом | 0,5 |  | 2 | Устный опрос, защита КР соответствующего варианта |
| Раздел 5. Защита информации в информационных системах | | | | | |
| 10 | Вредоносные программы и антивредоносное ПО. Управление логическим доступом | 1 |  | 4 | Устный опрос, защита КР соответствующего варианта |
| 11 | Основы построения криптосистем | - |  | 8 | Устный опрос, защита КР соответствующего варианта |
| 12 | Обеспечение безопасности в системах электронной коммерции | - |  | 4 | Устный опрос, защита КР соответствующего варианта |
| 13 | Противодействие атакам | - |  | 8 | Устный опрос, защита КР соответствующего варианта |
| Раздел 6. Основы управления интеллектуальной собственностью | | | | | |
| 14 | Авторское право и смежные права | 1 |  | 4 | Устный опрос, защита КР соответствующего варианта |
| 15 | Промышленная собственность | 1 |  | 4 | Устный опрос, защита КР соответствующего варианта |
| 16 | Патентные исследования | - | 2 | 6 | Тестирование, защита КР |
| 17 | Коммерческое использование объектов интеллектуальной собственности. Защита прав авторов и правообладателей | - |  | 4 | Устный опрос, защита КР соответствующего варианта |
|  | Текущая аттестация |  |  |  | зачет |
|  | Итого | 8 | 4 | 82 |  |

**3.4 Учебно-методическая карта учебной дисциплины в дистанционной форме обучения**

| Номер раздела, темы по п.1 | Название раздела, темы | Количество работ | | | Самостоятельная работа, часы | Форма контроля знаний студентов |
| --- | --- | --- | --- | --- | --- | --- |
| КР | ЛР | ИПР |
| Раздел 1. Методология информационной безопасности | | **1** |  |  |  | Защита КР |
| 1 | Основные понятия и определения в сфере защиты информации. Охраняемые сведения и их демаскирующие признаки. Классификация угроз ИБ и методов ЗИ |  |  | 4 |
| Раздел 2. Правовые и организационные методы защиты информации | |  |  |  |
| 2 | Государственное регулирование в сфере защиты информации |  |  | 4 |
| 3 | Нормативно-правовое обеспечение защиты информации в организации. Коммерческая тайна. Политика ИБ. |  |  | 6 |
| 4 | Организационные меры по защите информации |  |  | 6 |
| 5 | Социальный инжиниринг |  |  | 6 |
| Раздел 3. Защита информации от утечки по техническим каналам | |  |  |  |
| 6 | Классификация технических каналов утечки информации по физическим принципам возникновения |  |  | 4 |
| 7 | Защита речевой информации. Защита информации от утечки за счет побочных электромагнитных излучений и наводок. Выявление закладных устройств. | 1 |  | - | 6 |
| Раздел 4. Инженерно-техническая защита объектов от несанкционированного доступа | |  | - |  |
| 8 | Техническая укрепленность периметра защищаемого объекта. Системы охранно-пожарной сигнализации |  | - | 6 |
| 9 | Системы видеонаблюдения. Системы контроля и управления доступом |  |  | 4 |
| Раздел 5. Защита информации в информационных системах | |  | - |  |  |
| 10 | Вредоносные программы и антивредоносное ПО. Управление логическим доступом |  | - | 6 | Защита КР |
| 11 | Основы построения криптосистем |  |  | 6 |
| 12 | Обеспечение безопасности в системах электронной коммерции |  | - | 6 |
| 13 | Противодействие атакам |  | - | 6 |
| Раздел 6. Основы управления интеллектуальной собственностью | |  | - |  |
| 14 | Авторское право и смежные права |  |  | 6 |
| 15 | Промышленная собственность |  |  | 6 |
| 16 | Патентные исследования |  |  | 6 |
| 17 | Коммерческое использование объектов интеллектуальной собственности. Защита прав авторов и правообладателей |  |  | 6 |
|  | Текущая аттестация |  |  |  |  | зачет |
|  | Итого | **2** |  |  | **94** |  |

**3.6. Учебно-методическая карта учебной дисциплины**

**в вечерней форме обучения для получения высшего образования, интегрированного со средним специальным образованием**

| Номер раздела, темы по п.1 | Название раздела, темы | Количество аудиторных часов | | Самостоятельная работа, часы | Форма контроля знаний студентов |
| --- | --- | --- | --- | --- | --- |
| ЛК | ПЗ |
| Раздел 1. Методология информационной безопасности | | | | | |
| 1 | Введение. Основные понятия ИБ. Основные виды защищаемых сведений. Классификация угроз | 0,5 | 2 | 2 | Тестирование, опрос |
| Раздел 2. Правовые и организационные методы защиты информации | | | | | |
| 2 | Государственное регулирование в сфере защиты информации | 0,5 |  | 2 | Устный опрос |
| 3 | Нормативно-правовое обеспечение защиты информации в организации. Коммерческая тайна. Политика ИБ. | 1 | 2 | 2 | Тестирование, опрос |
| 4 | Организационные меры по защите информации | 1 |  | 4 | Устный опрос |
| 5 | Социальный инжиниринг | 0,5 |  | 2 | Устный опрос |
| Раздел 3. Защита информации от утечки по техническим каналам | | | | | |
| 6 | Классификация технических каналов утечки информации по физическим принципам возникновения | 1 |  | 2 | Устный опрос |
| 7 | Защита речевой информации. Защита информации от утечки за счет побочных электромагнитных излучений и наводок. Выявление закладных устройств | 1 | 2 | 2 | Тестирование, опрос |
| Раздел 4. Инженерно-техническая защита объектов от несанкционированного доступа | | | | | |
| 8 | Техническая укрепленность периметра защищаемого объекта. Системы охранно-пожарной сигнализации | 0,5 |  | 2 | Устный опрос |
| 9 | Системы видеонаблюдения. Системы контроля и управления доступом | 0,5 |  | 2 | Устный опрос |
| Раздел 5. Защита информации в информационных системах | | | | | |
| 9 | Вредоносные программы и антивредоносное ПО. Управление логическим доступом | 0,5 |  | 2 | Устный опрос |
| 11 | Основы построения криптосистем | 1 | 2 | 4 | Тестирование, опрос |
| 12 | Обеспечение безопасности в системах электронной коммерции | 1 |  | 4 | Устный опрос |
| 10 | Основы сетевой безопасности. | 1 |  | 4 | Устный опрос |
| Раздел 6. Основы управления интеллектуальной собственностью | | | | | |
| 13 | Авторское право и смежные права | - | - | перезачт |  |
| 14 | Промышленная собственность | - | - | Перезачт |  |
| 15 | Патентные исследования | - | - | перезачт |  |
| 16 | Коммерческое использование объектов интеллектуальной собственности. Защита прав авторов и правообладателей | - | - | Перезачт |  |
|  | Текущая аттестация |  |  |  | зачет |
|  | Итого | **10** | **8** | **34** |  |

**3.7. Учебно-методическая карта учебной дисциплины**

**в заочной форме обучения для получения высшего образования, интегрированного со средним специальным образованием**

| Номер раздела, темы по п.1 | Название раздела, темы | Количество аудиторных часов | | Самостоятельная работа, часы | Форма контроля знаний студентов |
| --- | --- | --- | --- | --- | --- |
| ЛК | ПЗ |
| Раздел 1. Методология информационной безопасности | | | | | |
| 1 | Основные понятия и определения в сфере защиты информации. Охраняемые сведения и их демаскирующие признаки. Классификация угроз ИБ и методов ЗИ | - | 2 | 2 | Тестирование, опрос, защита КР соответствующего варианта |
| Раздел 2. Организационные методы защиты информации | | | | | |
| 2 | Государственное регулирование в сфере защиты информации | - |  | 2 | Устный опрос, защита КР соответствующего варианта |
| 3 | Нормативно-правовое обеспечение защиты информации в организации. Коммерческая тайна. Политика ИБ. | 0,5 | 2 | 4 | Тестирование, опрос, защита КР соответствующего варианта |
| 4 | Организационные меры по защите информации | - |  | 4 | Устный опрос, защита КР соответствующего варианта |
| 5 | Социальный инжиниринг | - |  | 4 | Устный опрос, защита КР соответствующего варианта |
| Раздел 3. Защита информации от утечки по техническим каналам | | | | | |
| 6 | Классификация технических каналов утечки информации по физическим принципам возникновения | 0,5 |  | 2 | Устный опрос, защита КР соответствующего варианта |
| 7 | Защита речевой информации. Защита информации от утечки за счет побочных электромагнитных излучений и наводок. Выявление закладных устройств | - |  | 4 | Устный опрос, защита КР соответствующего варианта |
| Раздел 4. Инженерно-техническая защита объектов от несанкционированного доступа | | | | | |
| 8 | Техническая укрепленность периметра защищаемого объекта. Системы охранно-пожарной сигнализации | 0,5 |  | 4 | Устный опрос, защита КР соответствующего варианта |
| 9 | Системы видеонаблюдения. Системы контроля и управления доступом | 0,5 |  | 2 | Устный опрос, защита КР соответствующего варианта |
| Раздел 5. Защита информации в информационных системах | | | | | |
| 10 | Вредоносные программы и антивредоносное ПО. Управление логическим доступом | 0,5 |  | 4 | Устный опрос, защита КР соответствующего варианта |
| 11 | Основы построения криптосистем | 0,5 |  | 4 | Устный опрос, защита КР соответствующего варианта |
| 12 | Обеспечение безопасности в системах электронной коммерции | 0,5 |  | 4 | Устный опрос, защита КР соответствующего варианта |
| 13 | Противодействие атакам | 0,5 |  | 4 | Устный опрос, защита КР соответствующего варианта |
| Раздел 6. Основы управления интеллектуальной собственностью | | | | | |
| 14 | Авторское право и смежные права |  |  | перезачт |  |
| 15 | Промышленная собственность |  |  | Перезачт |  |
| 16 | Патентные исследования |  |  | перезачт |  |
| 17 | Коммерческое использование объектов интеллектуальной собственности. Защита прав авторов и правообладателей |  |  | Перезачт |
|  | Текущая аттестация |  |  |  | зачет |
|  | Итого | 4 | 4 | 44 |  |

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

ПО УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ

УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТЕЙ

|  |  |  |  |
| --- | --- | --- | --- |
| перечень  учебных дисциплин | кафедра, обеспечивающая учебную дисциплину | Предложения  об изменениях  в содержании  по изучаемой  учебной дисциплине | Подпись заведующего кафедрой,  обеспечивающей учебную дисциплину,  с указанием номера  протокола и  даты заседания кафедры |
| Системы и сети передачи данных. Защита информации в компьютерных сетях | ИРТ |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись  протокол № 4 от 02.11.2015 |
| Теоретические основы проектирования электронных систем безопасности | ПИКС |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись  протокол № 6 от 07.11.2015 |
| Безопасность в компьютерных сетях |  |
| Методы защиты информации | Инф. |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись  протокол № 6 от 09.11.2015 |
| Администрирование и программирование распределенных приложений | ИТАС |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись  протокол № 6 от 09.11.2015 |

Зав. кафедрой защиты информации Л.М. Лыньков