**Учреждение образования**

**«Гомельский государственный университет имени Франциска Скорины»**

**УТВЕРЖДАЮ**

Проректор по учебной работе

ГГУ имени Ф. Скорины

И.В. Семченко

 2017

Регистрационный № УД-\_\_\_\_\_\_\_\_\_\_\_\_/уч.

**ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ**

**Учебная программа для специальности**

**1-39 03 02 Программируемые мобильные системы**

**1-39 03 01 Электронные системы безопасности**

2017

Учебная программа составлена на основе типовой учебной программы «Основы защиты информации», утвержденной ведущим учреждением высшего образования «Белорусский государственный университет информатики и радиоэлектроники» 05 апреля 2016 г., регистрационный № ТД- I. 1347 /тип и учебного плана учреждения образования «Гомельский государственный университет им. Франциска Скорины» для специальности 1-39 03 02 Программируемые мобильные системы и 1-39 03 01 Электронные системы безопасности.

**СОСТАВИТЕЛЬ:**

С.И. Соколов, старший преподаватель кафедры общей физики учреждения образования «Гомельский государственный университет имени Франциска Скорины»

**РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:**

Кафедрой общей физики учреждения образования «Гомельский государственный университет имени Франциска Скорины»

(протокол № \_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_);

Научно-методическим советом учреждения образования «Гомельский государственный университет имени Франциска Скорины»

 (протокол № \_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_).

Пояснительная записка

Дисциплина государственного компонента цикла общепрофессиональных и специальных дисциплин.

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 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 **компетенции**:

*академические:*

1. АК-1 умение применять базовые научно-теоретические знания для решения теоретических и практических задач;
2. АК-2 владение системным и сравнительным анализом;
3. АК-3 владение исследовательскими навыками;
4. АК-4 умение работать самостоятельно;
5. АК-5 способность порождать новые идеи (обладание креативностью);
6. АК-6 владение междисциплинарным подходом при решении проблем
7. АК-7 обладание навыками, связанными с использованием технических устройств, управлением информацией и работой с компьютером;
8. АК-8 обладание навыками устной и письменной коммуникации;
9. АК-9 умение учиться, повышать свою квалификацию в течение всей жизни;
10. АК-10 способность использовать основные законы естественнонаучных дисци­плин в профессиональной деятельности;
11. АК-11 владение основными методами, способами и средствами получения, хра­нения, переработки информации с использованием компьютерной техники;
12. АК-14 умение на научной основе организовывать свой труд, самостоятельно оценивать результаты своей деятельности;

*социально-личностные:*

1. СЛК-1 обладание качествами гражданственности;
2. СЛК-2 способность к социальному взаимодействию;
3. СЛК-3 обладание способностью к межличностным коммуникациям;
4. СЛК-5 способность к критике и самокритике;
5. СЛК-6 умение работать в команде.

*профессиональные:*

1. ПК-21 умение пользоваться глобальными информационными ресурсами;
2. ПК-22 умение владеть современными средствами инфокоммуникаций.

Дисциплина «Основы защиты информации» включает в себя модуль «Основы управления интеллектуальной собственностью».

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.

Форма получения образования – дневное, 2 курс, 4 семестр. Общее количество часов – 94(2,5 зачетные единицы); аудиторное количество часов – 52, из них: лекции – 32, практические занятия – 18, управляемая самостоятельная работа – 2.Форма отчётности — зачет (4 семестр).

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

**Раздел 1. Методология информационной безопасности**

**Тема 1.1 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**

**Тема 2.1Государственное 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.

**Тема 2.2Нормативно­-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.

**Тема 2.3 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.

**Тема 2.4 Социальный инжиниринг**

Основные принципы воздействия. Техники социнжиниринга. Методы противодействия.

**Раздел 3. Защита информации от утечки по техническим каналам**

**Тема 3.1 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.

**Тема 3.2 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**

**Тема 4.1 Техническая укрепленность периметра защищаемого объекта.**

Системы охранно-пожарной сигнализации Интегральная система безопасности. Системы меха­нической защиты. Системы обнаружения. Виды дат­чиков. Средства пожарной сигнализации.

**Тема 4.2 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**

**Тема 5.1 Вредоносные программы и антивредоносное ПО.**

Методы программной защиты информации. Классификация вредоносных программ. Управление логическим доступом Защита от компьютерных вирусов и шпионажного ПО. Дискреционный метод организации разграничения доступа. Мандатный метод организации разграничения доступа.

**Тема 5.2 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.

**Тема 5.3 Обеспечение безопасности в системах электронной коммерции**

Идентификация, аутентификация и авторизация. Технологии аутентификации. 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.

**Тема 5.4 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**

**Тема 6.1 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.

**Тема 6.2 Промышленная собственность**

Объекты промышленной собственности. Субъекты права промышленной собственности. Система выдачи охранных документов. Условия патентоспособности объектов промышленной собственности.

**Тема 6.3 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.

**Тема 6.4 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.

**Учебно-методическая карта дисциплины**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер раздела, темы | Название раздела, темы | Количество аудиторных часов | количествочасов УСР | Формы контролязнаний |
| лекции | лабораторныезанятия | практические занятия |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Методология информационной безопасности** | **2** | **-** | **2** |  |  |
| **1.1** | **Основные понятия и определения в сфере защиты информации.** | **2** | - | **2** | - |  |
|  | 1. Охраняемые сведения и их демаскирующие признаки. Классификация угроз ИБ и методов ЗИ
2. Задачи в сфере обеспечения информационной без-опасности. Информация общего и ограниченного распространения.
3. Угрозы информационной безопасности. Классификация угроз безопасности по виду, происхождению, источникам и характеру возникновения.
4. Обеспечение доступности, конфиденциальности и целостности информации. Защита информации от случайных видов угроз.
 | 2 | - | 2 | - | Текущий контроль |
| **2** | **Правовые и организационные методы защиты информации** | **8** | **-** | **2** | **-** |  |
| **2.1** | **Государственное регулирование в сфере защиты информации** | **2** | - | - | **-** |  |
|  | 1. Информационные технологии и право. Основные законы РБ в области компьютерного права.
2. Правовая защита от компьютерных преступлений.
3. Государственное регулирование в области защиты информации.
4. Международные стандарты и рекомендации в области ИБ.
 | 2 | - | - | **-** | фронтальный опрос |
| **2.2** | **Нормативно-правовое обеспечение защиты информации в организации** | **2** | **-** | **2** | **-** |  |
|  | 1. Коммерческая тайна. Политика ИБ.
2. Основные принципы создания системы менеджмента информационной безопасности.
3. Анализ рисков. Отнесение сведений к коммерческой тайне и их защита.
4. Назначение и цель политики ИБ.
 | 2 | - | 2 | **-** | фронтальный опрос |
| **2.3** | **Организационные меры по защите информации** | **2** | **-** | **-** | - |  |
|  | 1. Защита информационных активов организации. Защита человеческих ресурсов перед наймом, во время и по окончании работы.
2. Организация безопасных зон и защита оборудования. Процедуры эксплуатации и рабочие обязанности.
3. Резервное копирование. Обращение с носителями информации и правила по обмену информацией.
4. Постоянный контроль. Обязанности пользователей.
 | 2 | - | - | - | фронтальный опрос |
| **2.4** | **Социальный инжиниринг** | **2** | **-** | **-** | **-** |  |
|  | 1. Основные принципы воздействия.
2. Техники социнжиниринга.
3. Методы противодействия.
 | 2 | - | - | **-** | фронтальный опрос |
| **3** | **Защита информации от утечки по техническим каналам** | **4** | **-** | **4** | **-** |  |
| **3.1** | **Классификация технических каналов утечки информации по физическим принципам возникновения.** | **2** | **-** | **2** | **-** |  |
|  | 1. Классификация каналов утечки информации. Особенности технических каналов утечки информации.
2. Акустический канал утечки информации.
3. Электромагнитный канал утечки информации.
4. Источники образования технических каналов утечки информации.
 | 2 | - | 2 | **-** | Текущий контроль |
| **3.2** | **Защита речевой информации.** | **2** | **-** | **2** | **-** |  |
|  | 1. Защита информации от утечки за счет побочных электромагнитных излучений и наводок. Выявление закладных устройств
2. Технические методы защиты информации. Организация защищенных помещений. Пассивные методы защиты информации: звукоизоляция, фильтрация, экранирование.
3. Активные методы защиты информации: акустическая маскировка речи, электромагнитное зашумление, защита проводных линий. Технические средства защиты. Виды технических средств несанкционированного доступа.
4. Классификация поисковых работ по выявлению закладных устройств. Метод нелинейной локации. Методы и технические средства выявления сигналов подслушивающих устройств.
 | 2 | - | 2 | **-** | фронтальный опрос |
| **4** | **Инженерно-техническая защита объектов от несанкционированного доступа** | **2** |  | **2** | **-** |  |
| **4.1** | **Техническая укрепленность периметра защищаемого объекта. Системы охранно-пожарной сигнализации** | **1** | **-** | **1** | **-** |  |
|  | 1. Системы охранно-пожарной сигнализации
2. Интегральная система безопасности.
3. Системы механической защиты.
4. Системы обнаружения. Виды датчиков. Средства пожарной сигнализации.
 | 1 | - | 1 | - | фронтальный опрос |
| **4.2** | **Численное дифференцирование и интегрирование** | **1** | **-** | **1** | **-** |  |
|  | 1. Системы видеонаблюдения.
2. Состав системы контроля и управления доступом.
3. Идентификация и аутентификация, основные технологии.
 | 1 | - | 1 | **-** | фронтальный опрос |
| **5** | **Защита информации в информационных системах** | **10** | **-** | **2** | **-** |  |
| **5.1** | **Вредоносные программы и антивредоносное ПО.**  | **2** | **-** | **-** | **-** |  |
|  | 1. Методы программной защиты информации. Классификация вредоносных программ.
2. Управление логическим доступом Защита от компьютерных вирусов и шпионажного ПО.
3. Дискреционный метод организации разграничения доступа.
4. Мандатный метод организации разграничения доступа.
 | 2 | - | - | **-** | фронтальный опрос |
| **5.2** | **Основы построения криптосистем** | **2** | **-** | **2** | **-** |  |
|  | 1. Классификация методов шифрования. Алгоритмы шифрования.
2. Ключевая информация. Криптографические протоколы. Хэш-функции. Протокол электронной подписи RSA. Электронно-цифровая подпись.
3. Инфраструктура открытых ключей. Контроль целостности информации.
 | 2 | - | 2 | **-** | фронтальный опрос |
| **5.3** | **Обеспечение безопасности в системах электронной коммерции** | **2** | **-** | **2** | **-** |  |
|  | 1. Идентификация, аутентификация и авторизация. Технологии аутентификации. Сервер аутентификации Kerberos.
2. Общая схема электронных платежных систем. Платежные средства. Обеспечение безопасности электронных платежей через сеть Internet: протоколы SSL (Secure Sockets Layer), SET (Secure Electronic Transaction).
3. Защита информации, хранящейся на рабочих станциях.
 | 2 | - | 2 | **-** | фронтальный опрос |
| **5.4** | **Противодействие атакам**  | **4** | **-** | **-** | **-** |  |
|  | 1. Основы сетевой безопасности.
2. Атаки в компьютерных сетях. Сетевые сервисы безопасности.
3. Межсетевые экраны. Системы обнаружения вторжений.
4. Виртуальные частные сети.
 | 4 | - | - | **-** | фронтальный опрос |
| **6** | **Основы управления интеллектуальной собственностью** | **8** | **-** | **4** | **-** |  |
| **6.1** | **Авторское право и смежные права** | **2** | **-** | **2** | **-** |  |
|  | 1. Понятие интеллектуальной собственности. Объекты авторского права и смежных прав. Ограничения имущественных прав.
2. Срок действия авторского права. Принципы и условия возникновения, реализации и защиты авторских и смежных прав.
3. Управление имущественными правами авторов и обладателей смежных прав на коллективной основе. Авторский договор.
 | 2 | - | 2 | **-** | фронтальный опрос |
| **6.2** | **Промышленная собственность** | **2** | **-** | **-** | **-** |  |
|  | 1. Объекты промышленной собственности. Субъекты права промышленной собственности.
2. Система выдачи охранных документов.
3. Условия патентоспособности объектов промышленной собственности.
 | 2 | - | - | **-** | фронтальный опрос |
| **6.3** | **Патентные исследования** | **2** | **-** | **2** | **-** |  |
|  | 1. Патентная информация, ее видовой состав и особенности.
2. Исследование технического уровня и тенденций развития объектов техники, их патентоспособности, патентной чистоты, конкурентоспособности.
3. Особенности проведения патентных исследований на стадиях и этапах жизненного цикла продукции.
 | 2 | - | 2 | **-** | фронтальный опрос |
| **6.4** | **Коммерческое использование объектов интеллектуальной собственности. Защита прав авторов и правообладателей**  | **-** |  | - | **2** |  |
|  | 1. Основные формы передачи прав на объекты интеллектуальной собственности.
2. Классификация договоров их структура и содержание. Лицензионный договор. Виды лицензий. Организация работ по продаже лицензий.
3. Договор уступки. Государственная регистрация договоров.
4. Защита прав авторов и правообладателей.
 | - |  | - | **2** | фронтальный опрос |
|  | **Всего часов** | **32** |  | **18** | **2** | **Зачет** |

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

***Примерный перечень тем практических занятий****.*

1. Изучение типового алгоритма описания информационной системы. Описание и классификация информационных ресурсов.
2. Изучение методик оценки необходимости защиты информационной системы и определения ожидаемых затрат на защиту информации.
3. Изучение методики специальных исследований при защите речевой информации
4. Изучение активного метода защиты информации от утечки по акустическим каналам, ознакомление с устройством защиты речевой информации.
5. Изучение пассивного метода защиты информации от утечки по электромагнитным каналам. Расчет параметров экрана электромагнитного излучения.
6. Изучение порядка организации выделенных помещений. Ознакомление с порядком и средствами проведения поисковых работ на обнаружение закладных устройств.
7. Изучение симметричного алгоритма шифрования данных.
8. Получение практических навыков составления и оформления авторского до-говора
9. Исследование структуры и состава патентных документов. Составление и оформление заявок на объекты промышленной собственности

***Компьютерное программное обеспечение***

1. Операционная программа Windows.
2. Программа для моделирования цифровых и аналоговых электронных схем Electronic Workbench 5.12.
3. Электронные таблицы MS Excel.

***Темы рефератов***

1. Основные формы передачи прав на объекты интеллектуальной собственности.
2. Классификация договоров их структура и содержание. Лицензионный договор. Виды лицензий. Организация работ по продаже лицензий.
3. Договор уступки. Государственная регистрация договоров.
4. Защита прав авторов и правообладателей.

**Методические рекомендации по организации и выполнению УСР**

**по дисциплине «Основы защиты информации»**

Самостоятельное изучение данных тем преследует следующие цели:

– овладеть основными понятиями, определениями,

– уметь проводить необходимые расчеты,

– самостоятельно анализировать полученные результаты, делать соответствующие выводы.

Для самостоятельного изучения выделяются следующие темы:

1. Коммерческое использование объектов интеллектуальной собственности. Защита прав авторов и правообладателей (2 часа).

**УЧЕБНАЯ ПРОГРАММА УСР**

***1 Тема «Коммерческое использование объектов интеллектуальной собственности.*** ***Защита прав авторов и правообладателей» – 2 часа.***

Цели: 1) овладеть основными понятиями и определениями по данной теме;

2) сформировать компетенцию в умении коммерческого использования объектов интеллектуальной собственности.

Виды заданий УСР с учетом модулей сложности:

А) *Задания, формирующие знания по учебному материалу на уровне узнавания:*

1 Составление глоссария основных определений.

2 Подготовка краткого конспекта по теме.

3 Структурирование материала в виде таблиц или схем.

1. Подготовка реферата по теме «Коммерческое использование объектов интеллектуальной собственности».

*Форма выполнения заданий* – индивидуальная.

*Форма контроля выполнения заданий* – устное сообщение и обсуждение (1, 2, 3 задания), реферат (4 задание).

Б) *Задания, формирующие компетенции на уровне воспроизведения*:

1 Формулировка основных понятий и определений.

1. Знание коммерческого использования объектов интеллектуальной собственности.
2. Знание защиты прав авторов и правообладателей.

*Форма выполнения заданий* – индивидуальная и групповая.

*Форма контроля выполнения заданий* – устный опрос, групповая консультация.

В) *Задания, формирующие компетенции на уровне применения полученных знаний*:

1 Составление обзора научной (научно-технической) литературы по заданной теме.

2 Подготовка докладов.

*Форма выполнения заданий* – индивидуальная и групповая.

*Форма контроля выполнения заданий* – коллоквиум.

*Литература*

1. Девянин, П. Н. Модели безопасности компьютерных систем : учебное пособие для студентов вузов специальностей "Компьютерная безопасность", "Комплексное обеспечение информационной безопасности автоматизированных систем" [и др.] / П. Н. Девянин. - Москва : Академия, 2005. – 144 с .
2. Защита информации : учебное пособие для студентов вузов по направлению подготовки инфокоммуникационные технологии и системы связи квалификации (бакалавр, магистр) / А.П. Жук, [и др.]. - Москва : РИОР :РИНФРА-М, 2015. – 392 с.

**КРИТЕРИИ ОЦЕНОК РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТА**

|  |  |
| --- | --- |
| Баллы | Показатели оценки |
| 1(один) | Отсутствие приращения знаний и компетентности в рамках образовательного стандарта. |
| 2(два) | Фрагментарные знания в рамках образовательного стандарта; знания отдельных литературных источников, рекомендованных учебной программой дисциплины; неумение использовать научную терминологию дисциплины, наличие в ответе грубых и логических ошибок; пассивность на практических и лабораторных занятиях, низкий уровень культуры исполнения заданий. |
| 3(три) | Недостаточно полный объем знаний в рамках образовательного стандарта; знание части основной литературы, рекомендованной учебной программой дисциплины; использование научной терминологии, изложение ответа на вопросы с существенными и логическими ошибками; слабое владение инструментарием учебной дисциплины, некомпетентность в решении стандартных (типовых) задач; неумение ориентироваться в основных теориях, концепциях и направлениях изучаемой дисциплины; пассивность на практических и лабораторных занятиях, низкий уровень культуры исполнения заданий. |
| 4(четыре) | Достаточный объем знаний в рамках образовательного стандарта; усвоение основной литературы, рекомендованной учебной программой дисциплины; использование научной терминологии, логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок; владение инструментарием учебной дисциплины, умение его использовать в решении стандартных (типовых) задач; умение под руководством преподавателя решать стандартные (типовые) задачи; умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им оценку; работа под руководством преподавателя на практических, лабораторных занятиях, допустимый уровень исполнения заданий. |
| 5(пять) | Достаточные знания в объеме учебной программы; использование научной терминологии, грамотное логически правильное изложение ответа на вопросы, умение делать выводы; владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач; способность самостоятельно принимать типовые решения в рамках учебной программы; усвоение основной литературы, рекомендованной учебной программой дисциплины; умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку; самостоятельная работа на практических, лабораторных занятиях, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий. |
| 6(шесть) | Достаточно полные и систематизированные знания в объеме учебной программы; использование необходимой научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обобщения и обоснованные выводы; владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач; способность самостоятельно применять типовые решения в рамках учебной программы; усвоение основной литературы, рекомендованной учебной программой дисциплины; умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку; активная самостоятельная работа на практических, лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий. |
| 7(семь) | Систематизированные, глубокие и полные знания по всем разделам учебной программы; использовании научной терминологии (в том числе на иностранном языке), грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения; владение инструментарием учебной дисциплины, умение его использовать в постановке и решении научных и профессиональных задач; свободное владение типовыми решениями в рамках учебной программы; усвоение основной и дополнительной литературы, рекомендованной учебной программой дисциплины; умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им аналитическую оценку; самостоятельная работа на практических, лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий. |
| 8(восемь) | Систематизированные, глубокие и полные знания по всем поставленным вопросам в объеме учебной программы; использовании научной терминологии (в том числе на иностранном языке), грамотное и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения; владение инструментарием учебной дисциплины (в том числе техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач; способность самостоятельно решать сложные проблемы в рамках учебной программы; усвоение основной и дополнительной литературы, рекомендованной учебной программой дисциплины; умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им аналитическую оценку; активная самостоятельная работа на практических, лабораторных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий. |
| 9(девять) | Систематизированные, глубокие и полные знания по всем разделам учебной программы; точное использовании научной терминологии (в том числе на иностранном языке), грамотное и логически правильное изложение ответа на вопросы; владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации в рамках учебной программы; полное усвоение основной и дополнительной литературы, рекомендованной учебной программой дисциплины; умение ориентироваться в теориях, концепциях и направлениях по изучаемой дисциплине и давать им аналитическую оценку; систематическая, активная самостоятельная работа на практических, лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий. |
| 10(десять) | Систематизированные, глубокие и полные знания по всем разделам учебной программы, а также по основным вопросам, выходящим за ее пределы; точное использовании научной терминологии (в том числе на иностранном языке), грамотное, логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации; полное и глубокое усвоение основной и дополнительной литературы по изучаемой учебной дисциплине; умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин; творческая самостоятельная работа на практических, лабораторных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий. |

***Рекомендуемая литература***

*Основная*

1. Астапенко, Г.Ф. Аппаратно-программные методы и средства защиты информации: пособие для студентов специальностей "Радиофизика", "Физическая электроника" / Г.Ф. Астапенко. - Минск : БГУ, 2009 . – 183 с .
2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие для студентов, обучающихся по направлению "Прикладная информатика" / Е. К. Баранова, А. В. Бабаш. - Москва : РИОР : ИНФРА-М, 2017. ­­­– 321 с.
3. Баранова, Е. К. Моделирование системы защиты информации : практикум : учебное пособие для студентов вузов по направлению "Прикладная информатика" / Е. К. Баранова, А.В. Бабаш. - Москва : РИОР : ИНФРА-М, 2015. – 120 с.
4. Галицкий, А. В. Защита информации в сети - анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. - Москва : ДМК ПРЕСС, 2004 . – 616 с .
5. Грушо, А. А. Теоретические основы компьютерной безопасности : учебное пособие для студентов вузов спец. "Информационная безопасность" [и др.] / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - Москва : Академия, 2009. – 272 с.
6. Девянин, П. Н. Модели безопасности компьютерных систем : учебное пособие для студентов вузов специальностей "Компьютерная безопасность", "Комплексное обеспечение информационной безопасности автоматизированных систем" [и др.] / П. Н. Девянин. - Москва : Академия, 2005. – 144 с .
7. Защита информации : учебное пособие для студентов вузов по направлению подготовки инфокоммуникационные технологии и системы связи квалификации (бакалавр, магистр) / А.П. Жук, [и др.]. - Москва : РИОР :РИНФРА-М, 2015. – 392 с.
8. Куприяв, А. И. Основы защиты информации : учебное пособие для студентов специальностей "Радиоэлектронные системы", "Средства радиоэлектронной борьбы", "Информационные системы и технологии" / А.И. Куприянов, А. В. Сахаров, В. А. Шевцов. I Москва : Академия. 2008. – 256 с.
9. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата: для студентов вузов, обучающихся по инженерно-техническим направлениям и специальностям / А. Б. Лось, А.Ю. Нестеренко, М.И. Рожков. - Москва : ЮРАЙТ, 2016. – 473 с.
10. Васильева, И.Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата: для студентов вузов, обучающихся по инженерно-техническим направлениям и специальностям / И.Н. Васильева. - Москва : ЮРАЙТ, 2016. – 349 с.
11. 11 .Мельников, В. П. Информационная безопасность и защита информации : учебное пособие для студентов вузов специальности "Информационные системы и технологии" / В. 11. Мельников, С. А. Клейменов, А. М. Петраков .- Москва : Академия, 2009 . – 336 с .
12. Романов, О. А. Организационное обеспечение информационной безопасности ; учебник для студентов вузов специальностей "Организация и технология защиты информации", "Комплексная защита объектов информации" направления подготовки "Информационная безопасность" [и др.] / О. А. Романов, С. А. Бабин, С. Г. Жданов. - Москва : Академия, 2008. – 192 с .
13. Современная компьютерная безопасность : теоретические основы, практические аспекты : учебное пособие / А.Ю. Щербаков [и др.]. - Москва : Книжный мир, 2009 . S 1 CD-ROM .

*Дополнительная*

1. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для студентов вузов по направлениям "Информационная безопасность", "Информатика и вычислительная техника" / П. Б. Хорев. - Москва :ФОРУМ, 2013. – 352 с .
2. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. - Москва: ДМК ПРЕСС, 2012. – 592 с.
3. Шачнев, А. И. Устройства и системы охранно-пожарной сигнализации : учебное пособие для учащихся проф.-техн.училищ / А. И. Шачнев. - Минск :Технопринт, 2004 . – 240 с .