

Документ подписан простой электронной подписью  
Информация о владельце:

ФИО: Худин Александр Николаевич

Должность: Ректор

Дата подписания: 26.01.2021 13:00:41

Уникальный программный ключ:

08303ad8de1c60b987361de7085acb509ac3da145741b561af0ee3e73a19

## МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

"Курский государственный университет"

Кафедра информационной безопасности

УТВЕРЖДЕНО

протокол заседания

Ученого совета от 24.04.2017 г., №10

### Рабочая программа дисциплины Основы кибербезопасности

Направление подготовки: 20.03.01 Техносферная безопасность

Профиль подготовки: Безопасность труда и технологических процессов

Квалификация: бакалавр

Индустрально-педагогический факультет

Форма обучения: очная

Общая трудоемкость 2 ЗЕТ

Виды контроля в семестрах:

зачет(ы) 6

#### Распределение часов дисциплины по семестрам

| Семестр<br>(<Курс>.<Семестр<br>на курсе>) | 6 (3.2) |    | Итого |    |
|---|---------|----|-------|----|
|   | УП      | РП |       |    |
| Неделя                                    | 16      |    |       |    |
| Вид занятий                               | УП      | РП | УП    | РП |
| Лекции                                    | 16      | 16 | 16    | 16 |
| Лабораторные                              | 16      | 16 | 16    | 16 |
| Итого ауд.                                | 32      | 32 | 32    | 32 |
| Контактная работа                         | 32      | 32 | 32    | 32 |
| Сам. работа                               | 40      | 42 | 40    | 42 |
| Итого                                     | 72      | 74 | 72    | 74 |

Рабочая программа дисциплины Основы кибербезопасности / сост. Гранкин Валерий Егорович, кандидат педагогических наук, доцент; Курск. гос. ун-т. - Курск, 2017. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 21 марта 2016 г. № 246 "Об утверждении ФГОС ВО по направлению подготовки 20.03.01 Техносферная безопасность (уровень бакалавриата)" (Зарегистрировано в Минюсте России 20 апреля 2016 г. № 41872)

Рабочая программа дисциплины "Основы кибербезопасности" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 20.03.01 Техносферная безопасность профиль Безопасность труда и технологических процессов

Составитель(и):

Гранкин Валерий Егорович, кандидат педагогических наук, доцент

© Курский государственный университет, 2017

**1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

|     |  |
|-----|--|
| 1.1 | Сформировать базовый уровень знаний, умений и владения навыками по обеспечению информационной безопасности информационных систем и информационных ресурсов профессиональной деятельности |
|-----|--|

**2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП**

|                    |     |
|--------------------|-----|
| Цикл (раздел) ООП: | ФТД |
|--------------------|-----|

**3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**ОПК-1: способностью учитывать современные тенденции развития техники и технологий в области обеспечения техносферной безопасности, измерительной и вычислительной техники, информационных технологий в своей профессиональной деятельности**

**Знать:**

Базовые понятия и содержание технологий обеспечения основ кибербезопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах, а так же процессы управления информационной безопасностью защищаемых объектов

Базовый комплекс мер по обеспечению основ информационной безопасности с учетом их правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности, возможных внешних воздействий, вероятных угроз и уровня развития технологий защиты информации и основные требования содержащиеся в нормативно- правовом обеспечении оборота сведений составляющих служебную и коммерческую тайну

Необходимые основы закрепленные в технической документации с учетом действующих нормативных и методических документов в области информационной безопасности, а так же алгоритмы решения типовых задач обеспечения информационной безопасности и к применению программных средств системного, прикладного и специального назначения

**Уметь:**

применять базовые методы анализа изучаемых явлений, процессов и проектных решений и использовать основные требования закрепленные в законах и подзаконных актов, при разработки ИТ- технологий требующих правовых решений в ситуациях, возникающих вследствие нарушения основных законных интересов граждан и организаций

проводить базовый анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов и проводить эксперименты по заданной методике, осуществлять обработку результатов, оценку погрешности и определять достоверность получаемых результатов

осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения основ кибербезопасности и способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью

**Владеть:**

навыками проведения экспериментов по заданной методике, осуществлять обработку результатов, оценку погрешности и определять достоверность получаемых результатов; способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения основ кибербезопасности

базовыми навыками, позволяющими разрабатывать предложения по совершенствованию основ системы управления информационной безопасностью и формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью

базовыми методом проведения анализа информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов и способностью проводить эксперименты по заданной методике, осуществлять обработку результатов, оценку погрешности и определять достоверность получаемых результатов

**4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

| Код занятия | Наименование разделов и тем  | Вид занятий | Семестр / Курс | Часов | Интеракт. |
|-------------|--|-------------|----------------|-------|-----------|
|             | <b>Раздел 1. Раздел 1. Введение</b>  | Раздел      |                |       |           |
| 1.1         | Базовые задачи кибербезопасности в автоматизированных системах   | Лек         | 6              | 2     | 0         |
| 1.2         | Лабораторная работа №1   | Лаб         | 6              | 2     | 0         |
| 1.3         | Основы файловой системы Требования к системам защиты информации.   | Ср          | 6              | 14    | 0         |
| 1.4         | Лабораторная работа №2   | Лаб         | 6              | 2     | 0         |
|             | <b>Раздел 2. Раздел 2. Специфика технологии защищенного документооборота- Методологические рекомендации по анализу режимов работы кибернетических систем</b> | Раздел      |                |       |           |

|     |  |        |   |   |   |
|-----|--|--------|---|---|---|
| 2.1 | Антивирусы и базовая защита электронного документооборота от не санкционированного доступа   | Лек    | 6 | 2 | 0 |
| 2.2 | Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз  | Лек    | 6 | 2 | 0 |
| 2.3 | Лабораторная работа №3   | Лаб    | 6 | 2 | 0 |
| 2.4 | Общая характеристика сетей и протоколов передачи данных  | Ср     | 6 | 8 | 0 |
| 2.5 | Лабораторная работа №4   | Лаб    | 6 | 2 | 0 |
| 2.6 | Лабораторная работа №5   | Лаб    | 6 | 2 | 0 |
|     | <b>Раздел 3. Раздел 3. Принципы построения системы кибербезопасности. Определение уязвимостей автоматизированных систем и выбор средств защиты. Формирование требований к построению систем криптографической и стеганографической защиты.</b> | Раздел |   |   |   |
| 3.1 | Общие требования к паролям симметричное и асимметричное шифрование   | Лек    | 6 | 2 | 0 |
| 3.2 | Лабораторная работа №6   | Лаб    | 6 | 2 | 0 |
| 3.3 | Электронная подпись  | Лек    | 6 | 2 | 0 |
| 3.4 | Основы стеганографии   | Лек    | 6 | 2 | 0 |
| 3.5 | Защищенные каналы данных облачные технологии и защищённый документооборота   | Ср     | 6 | 8 | 0 |
| 3.6 | Лабораторная работа №7   | Лаб    | 6 | 2 | 0 |
|     | <b>Раздел 4. Раздел 4. Киберпреступность и способы её предотвращения</b>   | Раздел |   |   |   |
| 4.1 | Нормативно-правовые акты и стандарты по основам кибербезопасности  | Лек    | 6 | 2 | 0 |
| 4.2 | Преступления в сфере информационных технологий   | Ср     | 6 | 6 | 0 |
| 4.3 | Анализ базовых положений ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"  | Лек    | 6 | 2 | 0 |
| 4.4 | Анализ примеров применения ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" в образовательных учреждениях  | Ср     | 6 | 4 | 0 |
| 4.5 | Рубежный контроль  | Лаб    | 6 | 2 | 0 |
| 4.6 | Промежуточный контроль   | Зачёт  | 6 | 2 | 0 |

## 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине «Основы кибербезопасности» рассмотрены и одобрены на заседании кафедры математического анализа и прикладной математики 13.04.2017 протокол №7 и являются приложением к рабочей программе.

### 5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточной аттестации по дисциплине «Основы кибербезопасности» рассмотрены и одобрены на заседании кафедры математического анализа и прикладной математики 13.04.2017 протокол

№7 и являются приложением к рабочей программе.

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 6.1. Рекомендуемая литература

#### 6.1.1. Основная литература

|      | Заглавие   | Эл. адрес   | Кол- |
|------|--|---|------|
| Л1.1 | Загинайлов Ю. Н. - Теория информационной безопасности и методология защиты информации - М.   Берлин: Директ-Медиа, 2015. | <a href="http://biblioclub.ru/index.php?page=book&amp;id=276557">http://biblioclub.ru/index.php?page=book&amp;id=276557</a> | 1    |
| Л1.2 | Загинайлов Ю. Н. - Основы информационной безопасности: курс визуальных лекций - М.   Берлин: Директ-Медиа, 2015.         | <a href="http://biblioclub.ru/index.php?page=book&amp;id=362895">http://biblioclub.ru/index.php?page=book&amp;id=362895</a> | 1    |

#### 6.1.2. Дополнительная литература

|      | Заглавие   | Эл. адрес   | Кол- |
|------|--|---|------|
| Л2.1 | Шаньгин В. Ф. - Информационная безопасность и защита информации: учебное пособие - Москва: ДМК Пресс, 2014.  | <a href="http://www.iprbookshop.ru/29257">http://www.iprbookshop.ru/29257</a> | 1    |
| Л2.2 | Прохорова О. В. - Информационная безопасность и защита информации: Учебник - Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. | <a href="http://www.iprbookshop.ru/43183">http://www.iprbookshop.ru/43183</a> | 1    |

#### 6.1.3. Методические разработки

|      | Заглавие  | Эл. адрес | Кол- |
|------|---|-----------|------|
| Л3.1 | Крыжевич Л. С. - Информационная безопасность: учеб.-метод. пособие для студ. ФФМИ Курск. гос. ун-та - Курск: [б. и., 2015]. |           | 1    |

### 6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

|    |  |
|----|--|
| Э1 | Crypt-Online - <a href="http://crypt-online.narod.ru/">http://crypt-online.narod.ru/</a>   |
| Э2 | Online decrypt/encrypt too - <a href="https://www.tools4noobs.com/online_tools/encrypt/">https://www.tools4noobs.com/online_tools/encrypt/</a> |
| Э3 | Steganography Online - <a href="http://stylesuxx.github.io/steganography/">http://stylesuxx.github.io/steganography/</a>                       |
| Э4 | Image Steganography - <a href="https://incoherency.co.uk/image-steganography/">https://incoherency.co.uk/image-steganography/</a>              |

#### 6.3.1 Перечень программного обеспечения

|          |  |
|----------|--|
| 7.3.1.1  | 206:   |
| 7.3.1.2  | Microsoft Windows 7 (Open License: 47818817)                                 |
| 7.3.1.3  | Microsoft Office Professional 2007 (Open License: 43219389)                  |
| 7.3.1.4  | Adobe Acrobat Reader DC (Бесплатное программное обеспечение)                 |
| 7.3.1.5  | 7-Zip (Свободная лицензия GNU LGPL)  |
| 7.3.1.6  | Google Chrome (Свободная лицензия BSD)                                       |
| 7.3.1.7  |  |
| 7.3.1.8  | 325:   |
| 7.3.1.9  | Microsoft Windows 7 (Open License: 47818817)                                 |
| 7.3.1.10 | Microsoft Office Professional 2007 (Open License: 43219389)                  |
| 7.3.1.11 | Adobe Acrobat Reader DC (Бесплатное программное обеспечение)                 |
| 7.3.1.12 | 7-Zip (Свободная лицензия GNU LGPL)  |
| 7.3.1.13 | Google Chrome (Свободная лицензия BSD)                                       |
| 7.3.1.14 | Зоркий Глаз (Проприетарное условно-бесплатное программное обеспечение)       |
| 7.3.1.15 | PDF Creator (Свободное программное обеспечение AGPL )                        |
| 7.3.1.16 | Resuva FREE (Проприетарное условно-бесплатное программное обеспечение )      |
| 7.3.1.17 | USB Flash Security (Условно-бесплатное программное обеспечение )             |
| 7.3.1.18 | Easy File Locker (Проприетарное условно-бесплатное программное обеспечение ) |

|  |   |
|--|---|
| 7.3.1.1<br>9   |   |
| 7.3.1.2<br>0   | 146:  |
| 7.3.1.2<br>1   | Microsoft Windows 7 (Open License: 47818817)  |
| 7.3.1.2<br>2   | Microsoft Office Professional 2007 (Open License: 43219389)   |
| 7.3.1.2<br>3   | Adobe Acrobat Reader DC (Бесплатное программное обеспечение)  |
| 7.3.1.2<br>4   | 7-Zip (Свободная лицензия GNU LGPL)   |
| 7.3.1.2<br>5   | Google Chrome (Свободная лицензия BSD)  |
| <b>6.3.2 Перечень информационных справочных систем</b> |   |
| 7.3.2.1  | ЭБС КГУ <a href="http://library-reader.kursksu.ru/">http://library-reader.kursksu.ru/</a>                   |
| 7.3.2.2  | ЭБС "IPRBooks" <a href="http://www.iprbookshop.ru/">http://www.iprbookshop.ru/</a>                          |
| 7.3.2.3  | ЭБС "Юрайт" <a href="https://www.biblio-online.ru/">https://www.biblio-online.ru/</a>                       |
| 7.3.2.4  | ЭБС "Университетская библиотечная система Online" <a href="http://biblioclub.ru/">http://biblioclub.ru/</a> |
| 7.3.2.5  | Электронная библиотека.- Режим доступа: <a href="http://elibrary.ru">http://elibrary.ru</a>                 |
| 7.3.2.6  | Система КонсультантПлюс : <a href="http://base.consultant.ru">http://base.consultant.ru</a>                 |

| <b>7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)</b> |  |
|---|--|
| 7.1   | Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групп-повых и индивидуальных консультаций, текущего контроля и промежуточной аттестации,   |
| 7.2   | 305000, Куркая область, г.Курск, ул. Радищева,д. № 33, 206.  |
| 7.3   | Комплекты учебных столов и стульев (28 шт)   |
| 7.4   | Доска ученическая (настенная) – 1 шт.  |
| 7.5   | Мультимедиа-проектор – 1 шт.   |
| 7.6   |  |
| 7.7   | Лаборатория информационной безопасности и вычислительных сетей: учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации,самостоятельной работы:  |
| 7.8   | 305000, Куркая область, г.Курск, ул. Радищева,д. № 33, 325.  |
| 7.9   | Моноблок LenovoC560 – 9 шт.  |
| 7.10  | Стенд информационный 1,4м*0,9м – 9 шт.   |
| 7.11  | Малогобаритный камуфлированный блокиратор работы сотовых телефонов и закладных устройств – 1 шт.   |
| 7.12  | Селективный обнаружитель цифровых радиоустройств ST062 – 1 шт.   |
| 7.13  | Устройство защиты объектов информатизации от утечки информации за счет ПЭМИН «Блокада» – 1 шт.   |
| 7.14  | Нелинейный локатор «Буклет-2» – 1 шт.  |
| 7.15  | Устройство МП—1А – 1 шт.   |
| 7.16  | Электронно-оптическое устройст-во для обнаружения любых типов оптических устройств «Гранат» – 1 шт.  |
| 7.17  | Программно-аппаратный комплекс «Соболь» – 1 шт.  |
| 7.18  | ИМФ-3 имитатор многофункциональный – 1 шт.   |
| 7.19  |  |
| 7.20  | Помещение для самостоятельной работы обучающихся – читальный зал, оснащенная компьютерной техникой с возможностью подключения к сети "Интернет" и с обеспечением доступа в электронную информационно-образовательную среду университета. Наборы демонстрационного оборудования и учебно-наглядных пособий, представленных комплектом мультимедийных презентаций. |
| 7.21  | 305000, Куркая область, г.Курск, ул. Радищева,д. № 33, 146.  |
| 7.22  | Столов – 61  |
| 7.23  | Посадочных мест – 162  |
| 7.24  | Компьютеров:   |
| 7.25  | Для пользователей – 40   |
| 7.26  | Для библиотекаря – 2   |

|      |  |
|------|--|
| 7.27 | Моноблоков MSI (27 ) - модель MS-A912, 2гб оперативной памяти, Athlon CPU D525 1.80GHz         |
| 7.28 | Моноблоков Asus (13) - модель ET2220I, 4гб оперативной памяти, Intel Core i3-3220 CPU 3.30 GHz |

### 8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Приступая к изучению курса, студентам рекомендуется ознакомиться с содержанием рабочей программы, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками, имеющимся на кафедре.

Изучение дисциплины требует систематического и последовательного накопления знаний, поэтому студентам рекомендуется перед очередной лекцией просмотреть по конспекту материал предыдущей. При затруднениях в восприятии материала следует обращаться к основным литературным источникам, к лектору (по графику его консультаций) или к преподавателю на занятиях.

Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы.

К каждой теме учебной дисциплины подобрана основная и дополнительная литература.

Основная литература - это учебники и учебные пособия.

Дополнительная литература - это монографии, сборники научных трудов, журнальные и газетные статьи, различные справочники, энциклопедии, интернет ресурсы.

В начале изучения курса, в учебнике или учебном пособии, рекомендуем в качестве основной или дополнительной литературы для освоения дисциплины, студенту рекомендуется проанализировать оглавление, научно-справочный аппарат, аннотацию и предисловие.

Студенту рекомендуется использовать следующие виды записей при работе с литературой:

Конспект - краткая схематическая запись основного содержания научной работы, целью которой является не переписывание материала, а выявление его логики, системы доказательств, основных выводов. Тезисы - концентрированное изложение основных положений прочитанного материала.

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

Для изучения конспекта лекции в тот же день, после лекции студенту рекомендуется 10-15 минут.

Изучение конспекта лекции по предыдущей теме за день перед лекцией по следующей темой - 10-15 минут.

Изучение теоретического материала по учебнику и конспекту - 1 час в неделю.

Подготовка к лабораторному занятию - 30 мин.

Всего в неделю - 2 часа 55 минут.

При изучении дисциплины рекомендуется самостоятельно изучать материал, который еще не прочитан на лекции. В этом случае, понимание лекционного материала осуществляется студентом более эффективно.

Для понимания материала и качественного его усвоения рекомендуется следующая последовательность действий:

После работы на лекции, или на лабораторной работе, и после окончания учебных занятий, студенту рекомендуется самостоятельно проанализировать лекционный материал, или материал лабораторной работы (10-15 минут).

При подготовке к лекции, или лабораторной работе по следующей теме, студенту рекомендуется проанализировать лекционный материал, или материал лабораторной работы по предыдущей теме (10-15 минут).

При подготовке к лабораторным занятиям рекомендуется также изучить соответствующий теоретический материал по основам кибербезопасности, предусмотренный темой лабораторной работы.

В течение учебной недели студенту рекомендуется изучать материал по основам кибербезопасности, изложенный в рекомендуемой литературе в течение 1 часа.