

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Худин Александр Николаевич

Должность: Ректор

Дата подписания: 01.02.2021 12:32:42

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: 38.05.02 Таможенное дело

Профиль подготовки: Таможенное декларирование и таможенные платежи

Квалификация: специалист

Факультет экономики и менеджмента

Форма обучения: очная

Общая трудоемкость 2 ЗЕТ

Виды контроля в семестрах:

зачет(ы) 6

Распределение часов дисциплины по семестрам

| Семестр (<Курс>.<Семестр на курсе>) | 6 (3.2) | | Итого | |
|---|---------|----|-------|----|
| | уп | рп | | |
| Неделя | 18 | | уп | рп |
| Вид занятий | уп | рп | уп | рп |
| Лекции | 18 | 18 | 18 | 18 |
| Лабораторные | 18 | 18 | 18 | 18 |
| Итого ауд. | 36 | 36 | 36 | 36 |
| Контактная работа | 36 | 36 | 36 | 36 |
| Сам. работа | 36 | 38 | 36 | 38 |
| 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 17 августа 2015 г. № 850 "Об утверждении ФГОС ВО по специальности 38.05.02 Таможенное дело (уровень специалитета)" (Зарегистрировано в Минюсте России 09 сентября 2015 г. № 38864)

Рабочая программа дисциплины "Основы кибербезопасности" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 38.05.02 Таможенное дело профиль Таможенное декларирование и таможенные платежи

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 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Знать:

основные 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

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

проводить 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 решения и поиска необходимых процессов в управлении информационной безопасностью защищаемых объектов, а также поиском и применением нормативно-правовой базы для решения конкретных задач обеспечения законности в сфере информационной безопасности

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

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. |
|-------------|---|-------------|----------------|-------|-----------|
| | Раздел 1. Раздел 1. Введение | Раздел | | | |
| 1.1 | Базовые задачи кибербезопасности в автоматизированных системах | Лек | 6 | 2 | 0 |
| 1.2 | Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз | Лек | 6 | 2 | 0 |
| 1.3 | Лабораторная работа №1 | Лаб | 6 | 2 | 0 |
| 1.4 | Основы файловой системы Требования к системам защиты информации. | Ср | 6 | 10 | 0 |
| 1.5 | Лабораторная работа №2 | Лаб | 6 | 2 | 0 |

| | | | | | |
|-----|--|--------|---|---|---|
| | Раздел 2. Раздел 2. Специфика технологии защищенного документооборота- Методологические рекомендации по анализу режимов работы кибернетических систем | Раздел | | | |
| 2.1 | Антивирусы и базовая защита электронного документооборота от не санкционированного доступа | Лек | 6 | 2 | 0 |
| 2.2 | Лабораторная работа №3 | Лаб | 6 | 2 | 0 |
| 2.3 | Общая характеристика сетей и протоколов передачи данных | Ср | 6 | 6 | 0 |
| 2.4 | Лабораторная работа №4 | Лаб | 6 | 2 | 0 |
| 2.5 | Лабораторная работа №5 | Лаб | 6 | 2 | 0 |
| | 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. | Раздел | | | |
| 3.1 | Общие требования к паролям симметричное и асимметричное шифрование | Лек | 6 | 2 | 0 |
| 3.2 | Основы стеганографии | Лек | 6 | 2 | 0 |
| 3.3 | Лабораторная работа №6 | Лаб | 6 | 2 | 0 |
| 3.4 | Электронная подпись | Лек | 6 | 2 | 0 |
| 3.5 | Хэш-функция как основа защиты информации при электронном документообороте | Лек | 6 | 2 | 0 |
| 3.6 | Защита информации средствами стеганографии с помощью прикладного программного обеспечения | Ср | 6 | 4 | 0 |
| 3.7 | Защищенные каналы данных облачные технологии и защищённый документооборота | Ср | 6 | 8 | 0 |
| 3.8 | Лабораторная работа №7 | Лаб | 6 | 2 | 0 |
| 3.9 | Лабораторная работа №8 | Лаб | 6 | 2 | 0 |
| | Раздел 4. Раздел 4. Киберпреступность и способы её предотвращения | Раздел | | | |
| 4.1 | Нормативно-правовые акты и стандарты по основам кибербезопасности | Лек | 6 | 2 | 0 |
| 4.2 | Анализ базовых положений ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" | Лек | 6 | 2 | 0 |
| 4.3 | Преступления в сфере информационных технологий | Ср | 6 | 4 | 0 |
| 4.4 | Анализ примеров практического применения ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" в образовательных учреждениях | Ср | 6 | 4 | 0 |
| 4.5 | Лабораторная работа №9 | Лаб | 6 | 2 | 0 |
| 4.6 | Промежуточная аттестация | 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. - Основы информационной безопасности: курс визуальных лекций - М. Берлин: Директ-Медиа, 2015. | http://biblioclub.ru/index.php?page=book&id=362895 | 1 |
| Л1.2 | Загинайлов Ю. Н. - Теория информационной безопасности и методология защиты информации - М. Берлин: Директ-Медиа, 2015. | http://biblioclub.ru/index.php?page=book&id=276557 | 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. | http://www.iprbookshop.ru/29257 | 1 |
| Л2.2 | Прохорова О. В. - Информационная безопасность и защита информации: Учебник - Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. | http://www.iprbookshop.ru/43183 | 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 - http://crypt-online.narod.ru/ |
| Э2 | Online decrypt/encrypt tool - https://www.tools4noobs.com/online_tools/encrypt/ |
| Э3 | Steganography Online - http://stylesuxx.github.io/steganography/ |
| Э4 | Image Steganography - https://incoherency.co.uk/image-steganography/ |

6.3.1 Перечень программного обеспечения

| | |
|----------|--|
| 7.3.1.1 | 501: |
| 7.3.1.2 | Microsoft Windows XP Professional Open License: 47818817), |
| 7.3.1.3 | Microsoft Office 2003 Suites Open Open License: 41902857 |
| 7.3.1.4 | Adobe Acrobat Reader DC Бесплатное программное обеспечение |
| 7.3.1.5 | GoogleChromeСвободная лицензияBSD; |
| 7.3.1.6 | 7-Zip (Свободная лицензия GNU LGPL) |
| 7.3.1.7 | |
| 7.3.1.8 | 505: |
| 7.3.1.9 | Microsoft Windows 7 Professional (Open License: 47818817) |
| 7.3.1.10 | Microsoft Office Professional Plus 2007 (Open License: 43219389) |
| 7.3.1.11 | Google Chrome Свободная лицензия BSD. |
| 7.3.1.12 | Adobe Acrobat Reader DC Бесплатное программное обеспечение |
| 7.3.1.13 | 7-Zip (Свободная лицензия GNU LGPL) |
| 7.3.1.14 | |
| 7.3.1.15 | 303: |

| | |
|--|---|
| 7.3.1.1 6 | Microsoft Windows 8 Prof (Open License: 47818817); |
| 7.3.1.1 7 | Microsoft Office Professional Plus 2007 (Open License: 43219389); |
| 7.3.1.1 8 | 7-Zip (Свободная лицензия GNU LGPL); |
| 7.3.1.1 9 | Adobe Acrobat Reader DC (Бесплатное программное обеспечение); |
| 7.3.1.2 0 | Google Chrome (Свободная лицензия BSD); |
| 6.3.2 Перечень информационных справочных систем | |
| 7.3.2.1 | ЭБС КГУ http://library-reader.kursksu.ru/ |
| 7.3.2.2 | ЭБС "IPRBooks" http://www.iprbookshop.ru/ |
| 7.3.2.3 | ЭБС "Юрайт" https://www.biblio-online.ru/ |
| 7.3.2.4 | ЭБС "Университетская библиотечная система Online" http://biblioclub.ru/ |
| 7.3.2.5 | Электронная библиотека.- Режим доступа: http://elibrary.ru |
| 7.3.2.6 | Система КонсультантПлюс : http://base.consultant.ru |

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

| | |
|------|--|
| 7.1 | Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, |
| 7.2 | 305000, Курская область, г. Курск, ул. Радищева, д. № 29, ауд. 501 |
| 7.3 | Парта первого ряда двухместная – 2 шт. |
| 7.4 | Парта первого ряда трехместная – фанера – 9 шт. |
| 7.5 | Парта последнего ряда двухместная – 2 шт. |
| 7.6 | Парта последнего ряда одноместная – 1 шт. |
| 7.7 | Парта последнего ряда трехместная – фанера – 8 шт. |
| 7.8 | Парта среднего ряда двухместная – 6 шт. |
| 7.9 | Парта среднего ряда одноместная – 1 шт. |
| 7.10 | Парта среднего ряда трехместная – фанера – 26 шт. |
| 7.11 | Доска аудиторная – 1 шт. |
| 7.12 | Стол офисный угловой с приставной тумбой– 1 шт. |
| 7.13 | Переносной мультимедийный проектор Optoma DX 211 (DLP. 2500Lm.XGA.3500: 1 |
| 7.14 | Мобильный ПК EMACHINES E510 – 1 шт. |
| 7.15 | |
| 7.16 | |
| 7.17 | Лаборатория технологий управления и торгового дела |
| 7.18 | 305000, Курская область, г. Курск, ул. Радищева, д. № 29, 505 |
| 7.19 | Доска магнитно-маркерная 90*120 PROFF WB0912/20-0702 (с магнитом и марке-ром) – 1 шт., |
| 7.20 | Доска информационная – 1 шт., |
| 7.21 | Концентратор Switch 24 port COMPEX – 1 шт., |
| 7.22 | Стол офисный угловой с подкатной тумбой 140*140/65*75 – 1 шт., |
| 7.23 | Стол компьютерный 103*67*75 – 11 шт., |
| 7.24 | Кресло рабочее поворотное-подъемное Chairman CH 661 – 13 шт., |
| 7.25 | Компьютер МК 2012-3400-4-8 (с/бл, монит, клав., акуст. система) – 12 шт., |
| 7.26 | Огнетушитель ОУ-3 – 1 шт., |
| 7.27 | Стул полумягкий ERA – 4 шт. |
| 7.28 | |
| 7.29 | Учебная аудитория для самостоятельной работы студентов, 305000, Курская область, |
| 7.30 | г. Курск, ул. Радищева, д. № 29, 303 |
| 7.31 | Стол – 55, |
| 7.32 | Стул – 55, |
| 7.33 | Компьютеров – 28 |

| | |
|------|---|
| 7.34 | Моноблоков ASUS ET220I All-in-one PC, Intel Core i3-322; NVG T630 1 Гб, Память 4 Гб; CPU 3.30 GHz; HDD 1 Тб, DVD-RW |
|------|---|

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, рекомендуемом 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.