ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КОМПЬЮТЕРНЫХ СИСТЕМ И ТЕХНОЛОГИЙ

ОДОБРЕНО УМС ИИКС  
  
Протокол № УМС-575/08-1   
  
от 28.08.2020 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

ЗАЩИТА ИНФОРМАЦИИ (ДОПОЛНИТЕЛЬНЫЕ ГЛАВЫ)

|  |  |
| --- | --- |
| Направление подготовки (специальность) | 09.03.01 Информатика и вычислительная техника |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Семестр** | **Трудоемкость, кред.** | **Общий объем курса, час.** | **Лекции, час.** | **Практич. занятия, час.** | **Лаборат. работы, час.** | **СРС, час.** | **КСР, час.** | **Форма(ы) контроля, экз./зач./КР/КП** |

АННОТАЦИЯ

Дисциплина посвящена изучению дополнительных глав по курсу Защита информации, предусмотрено изучение семи учебных тем.

Отмечается важность и сложность противодействия информационно-психологическому воздействию, атакам на компьютерные системы без использования технических средств. Рассматриваются методы защиты информации (ЗИ) от случайных деструктивных воздействий. Подробно рассматриваются методы защиты от активного противника, способного менять состояние атакуемой системы. Изучаются основы теории конечных полей, основы эллиптической криптографии.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью дисциплины «Защита информации (дополнительные главы)» является формирование у студентов знаний и представлений о методах защиты информации (ЗИ) от случайных деструктивных воздействий, о методах контролепригодного проектирования цифровой аппаратуры, методах защиты информации, пересылаемой по каналам связи, о стохастических методах ЗИ, а также о математических основах криптологии.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Защита информации (дополнительные главы)» относится к вариативным дисциплинам профессионального цикла направления 09.03.01. Приобретенные знания позволят студентам в своей будущей профессиональной деятельности безопасно использовать ключевые IT-технологии цифровой экономики.

С точки зрения организации учебного процесса дисциплина связана со следующими дисциплинами ООП бакалавра, предусмотренными учебным планом:

 "Защита информации";

 "Схемотехника ЭВМ";

 "Низкоуровневое программирование";

 "Программирование на языке высокого уровня".

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

|  |  |
| --- | --- |
| Код и наименование компетенции | Код и наименование индикатора достижения компетенции |

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п.п** | **Наименование раздела учебной дисциплины** | **Недели** | **Лекции/ Практ. (семинары )/ Лабораторные работы, час.** | **Обязат. текущий контроль (форма\*, неделя)** | **Максимальный балл за раздел\*\*** | **Аттестация раздела (форма\*, неделя)** | **Индикаторы освоения компетенции** |

\* – сокращенное наименование формы контроля

\*\* – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

|  |  |
| --- | --- |
| **Обозначение** | **Полное наименование** |
| КИ | Контроль по итогам |

КАЛЕНДАРНЫЙ ПЛАН

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Недели** | **Темы занятий / Содержание** | **Лек., час.** | **Пр./сем., час.** | **Лаб., час.** |

Сокращенные наименования онлайн опций:

|  |  |
| --- | --- |
| **Обозначение** | **Полное наименование** |
| ЭК | Электронный курс |
| ПМ | Полнотекстовый материал |
| ПЛ | Полнотекстовые лекции |
| ВМ | Видео-материалы |
| АМ | Аудио-материалы |
| Прз | Презентации |
| Т | Тесты |
| ЭСМ | Электронные справочные материалы |
| ИС | Интерактивный сайт |

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При изучении тем дисциплины «Защита информации (дополнительные главы)» используются различные образовательные технологии – во время аудиторных занятий читаются лекции с использованием ПК и мультимедийного проектора. Самостоятельная работа студентов предполагает участие преподавателей, осуществляющих чтение лекций, ведение практических занятий по данной дисциплине (консультации, помощь в написании тестов и т.д.) и индивидуальную работу студента в библиотеке и компьютерном классе.

Методы обучения, применяемые при освоении дисциплины, способствуют закреп-лению и углублению знаний, овладению умениями и получению навыков в предметной области. Содержание учебного плана диктует выбор методов обучения:

 информационно-развивающие – объяснение, демонстрация, решение задач, само-стоятельная работа с рекомендуемой литературой;

 проблемно-поисковые и исследовательские – самостоятельная проработка предла-гаемых или самостоятельно формулируемых вопросов предметной области.

 использование методологии сильного мышления при разрешении технических противоречий, возникающих при решении задач ЗИ;

 проверка остаточных знаний и тестирование.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

|  |  |
| --- | --- |
| **Компетенция** | **Индикаторы освоения** |

Оценочные средства приведены в Приложении.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ И20 Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие для вузов, Москва: НИЯУ МИФИ, 2012

2. ЭИ Ч-45 Применение искусственных нейронных сетей и системы остаточных классов в криптографии : учебное пособие, Москва: Физматлит, 2012

3. ЭИ Р17 Разрушающие программные воздействия : учебно-методическое пособие для вузов, ред. М. А. Иванов, Москва: НИЯУ МИФИ, 2011

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 Р17 Разрушающие программные воздействия : учебно-методическое пособие для вузов, А. Б. Вавренюк [и др.], Москва: НИЯУ МИФИ, 2011

2. 004 П64 Поточные шифры : , А.В.Асосков [и др.], М.: Кудиц-образ, 2003

3. 004 Ш76 Секреты и ложь : Безопасность данных в цифровом мире, Б. Шнайер, М.и др.: Питер, 2003

4. 004 Г82 Цифровая стеганография : , В. Г. Грибунин, И. Н. Оков, И. В. Туринцев, М.: Солон-Пресс, 2002

5. 0 М24 Современная криптография : теория и практика, В. Мао, Москва [и др.]: Вильямс, 2005

6. 004 И20 Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие для вузов, М. А. Иванов, И. В. Чугунков ; ред. : М. А. Иванов, Москва: НИЯУ МИФИ, 2012

7. 004 И20 Теория, применение и оценка качества генераторов псевдослучайных последовательностей : , М.А. Иванов, И.В. Чугунков, Москва: Кудиц-образ, 2003

8. 0 В24 Введение в криптографию : Новые математические дисциплины, Под ред. В.В. Ященко, СПб и др.: МЦНМО; Питер, 2001

9. 519 С13 Введение в алгебраические коды : учебное пособие, Ю. Л. Сагалович, Москва: ИППИ, 2010

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Приведены в приложении

Автор(ы):

|  |  |  |
| --- | --- | --- |
|  | Иванов Михаил Александрович, д.т.н., профессор |  |

Рецензент(ы):

|  |  |  |
| --- | --- | --- |
|  | Чугунков И.В. |  |