ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КОМПЬЮТЕРНЫХ СИСТЕМ И ТЕХНОЛОГИЙ

ОДОБРЕНО

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

|  |  |
| --- | --- |
| Направление подготовки (специальность) | 09.04.01 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** |
| 1 | 3-5 | 108-180 | 32 | 0 | 16 | 24-96 | 0 | Э |
| Итого | 3-5 | 108-180 | 32 | 0 | 16 | 24-96 | 0 |  |

АННОТАЦИЯ

Формирование принципов построения защищенных компьютерных систем, в том числе критически важных (ядерная энергетика, оборона, космос) компьютерных систем.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины являются изучение принципов построения защищенных компьютерных систем, в том числе критически важных (ядерная энергетика, оборона, космос) компьютерных систем.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина Защита информации относится к базовой части рабочего учебного плана.

Для успешного освоения дисциплины Защита информации необходимы компетенции, формируемые в результате освоения следующих дисциплин:

ЭВМ и периферийные устройства

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** |
|  | *1 Семестр* |  |  |  |  |  |  |
| 1 | Защита информации от умышленных деструктивных воздействий | 1-8 | 16/0/8 |  | КИ-8 | 25 |  |
| 2 | Защита информации от случайных деструктивных воздействий | 9-16 | 16/0/8 |  | КИ-16 | 25 |  |
|  | *Итого за 1 Семестр* |  | 32/0/16 |  |  | 50 |  |
|  | **Контрольные мероприятия за 1 Семестр** |  |  |  | Э | 50 |  |

\* – 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 |
| Э | Экзамен |

КАЛЕНДАРНЫЙ ПЛАН

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Недели** | **Темы занятий / Содержание** | **Лек., час.** | **Пр./сем., час.** | **Лаб., час.** |
|  | *1 Семестр* | 32 | 0 | 16 |
| **1-8** | **Защита информации от умышленных деструктивных воздействий** | 16 | 0 | 8 |
| 1 | Компьютерные системы (КС) как объекты защиты информации. Методы и средства защиты информации от случайных и преднаме-ренных деструктивных воздействий. Требования к эффективной системе обеспечения безопасности информации (ОБИ). | Всего аудиторных часов | Всего аудиторных часов | Всего аудиторных часов |
| 2 |  | 1 |
| Онлайн | Онлайн | Онлайн |
|  |  |  |
| 2 | Введение в криптологию. Основные термины и определения. Криптографическое преобразование информации. Классификация шифров. Требования к качественному шифру. Требования к каче-ственной хеш-функции. | Всего аудиторных часов | Всего аудиторных часов | Всего аудиторных часов |
| 2 |  | 1 |
| Онлайн | Онлайн | Онлайн |
|  |  |  |
| 3 | Криптосистемы с секретным ключом. ГОСТ 28147-89. Американ-ский стандарт криптозащиты AES-128. Поточные шифры A5, RC4. | Всего аудиторных часов | Всего аудиторных часов | Всего аудиторных часов |
| 2 |  | 1 |
| Онлайн | Онлайн | Онлайн |
|  |  |  |
| 4 - 5 | Криптосистемы с открытым ключом. Криптосистема RSA. Ранцевая криптосистема. | Всего аудиторных часов | Всего аудиторных часов | Всего аудиторных часов |
| 4 |  | 2 |
| Онлайн | Онлайн | Онлайн |
|  |  |  |
| 6 - 8 | Криптографические протоколы. Протокол выработки общего сек-ретного ключа. Протоколы электронной цифровой подписи. Про-токолы аутентификации удаленных абонентов. Протоколы доказа-тельства с нулевым разглашением знаний. Протоколы разделения секрета. | Всего аудиторных часов | Всего аудиторных часов | Всего аудиторных часов |
| 6 |  | 3 |
| Онлайн | Онлайн | Онлайн |
|  |  |  |
| **9-16** | **Защита информации от случайных деструктивных воздействий** | 16 | 0 | 8 |
| 9 | Цифровые деньги. Структура централизованной платежной систе-мы. Жизненный цикл цифровой купюры. | Всего аудиторных часов | Всего аудиторных часов | Всего аудиторных часов |
| 2 |  | 1 |
| Онлайн | Онлайн | Онлайн |
|  |  |  |
| 10 - 11 | Стохастические методы защиты информации. Теория, применение и оценка качества генераторов псевдослучайных чисел (ГПСЧ). Внесение неопределенности в работу средств и объектов защиты. Функции ГПСЧ и хеш-генераторов в системах ОБИ. | Всего аудиторных часов | Всего аудиторных часов | Всего аудиторных часов |
| 4 |  | 2 |
| Онлайн | Онлайн | Онлайн |
|  |  |  |
| 12 | Разрушающие программные воздействия (РПВ). Структура ком-плекса программных средств антивирусной защиты. Методы анти-вирусной защиты. | Всего аудиторных часов | Всего аудиторных часов | Всего аудиторных часов |
| 2 |  | 1 |
| Онлайн | Онлайн | Онлайн |
|  |  |  |
| 13 | Контроль целостности информации. CRC-коды. Криптографиче-ские методы контроля целостности информации. | Всего аудиторных часов | Всего аудиторных часов | Всего аудиторных часов |
| 2 |  | 1 |
| Онлайн | Онлайн | Онлайн |
|  |  |  |
| 14 - 16 | Разграничение доступа. Организация парольных систем. | Всего аудиторных часов | Всего аудиторных часов | Всего аудиторных часов |
| 6 |  | 3 |
| Онлайн | Онлайн | Онлайн |
|  |  |  |

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 |

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

|  |  |
| --- | --- |
| **Недели** | **Темы занятий / Содержание** |
|  | *1 Семестр* |
|  | ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ РАБОТ    Работа 1. Криптоанализ шифра "Усложненная перестановка по таблице".  Работа 2. Протоколы электронной цифровой подписи.  Работа 3. Российский стандарт криптозащиты ГОСТ 28147-89.  Работа 4. Американский стандарт криптозащиты AES. |
| 4 - 5 | Работа 1. Криптоанализ шифра "Усложненная перестановка по таблице". |
| 5 - 7 | Работа 2. Протоколы электронной цифровой подписи. |
| 8 - 9 | Работа 3. Российский стандарт криптозащиты ГОСТ 28147-89. |
| 10 - 11 | Работа 4. Американский стандарт криптозащиты AES. |

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При чтении лекционного материала используется электронное сопровождение курса: справочно-иллюстративный материал воспроизводится и озвучивается в аудитории с использованием проектора и переносного компьютера в реальном времени. Электронный материал доступен студентам для использования и самостоятельного изучения на сайте кафедры по адресу http://dozen.mephi.ru.

На сайте кафедры также находится методический и справочный материал, необходимый для проведения лабораторного практикума по курсу.

Лабораторный практикум проводится по расписанию в дисплейном классе одновременно для группы студентов, работающих в интерактивном режиме. Допустимо выполнение лабораторных работ в составе локальной сети кафедры или в удаленном режиме, используя Интернет.

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

Автор(ы):

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

Рецензент(ы):

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