|  |  |  |  |
| --- | --- | --- | --- |
| МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  РОССИЙСКОЙ ФЕДЕРАЦИИ  ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  «Национальный исследовательский ядерный университет «МИФИ»  Озерский технологический институт -  филиал федерального государственного автономного образовательного учреждения  высшего образования «Национальный исследовательский ядерный университет «МИФИ»  (ОТИ НИЯУ МИФИ) | | | |
| Кафедра прикладной математики | | |
| УТВЕРЖДАЮ  ДИРЕКТОР  И. А. Иванов  «\_\_» \_\_\_\_ 2021 г. | | |
| РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ | | |
| Защита данных | | |
| (наименование дисциплины) | | |
|  | | |
| Направление подготовки (специальность): | 12.03.01 Приборостроение | |
|  |  | |
| Профиль подготовки: | Программное обеспечение и информационно-измерительные технологии в приборостроении | |
|  |  | |
| Наименование образовательной программы: | Программное обеспечение и информационно-измерительные технологии в приборостроении | |
|  |  | |
| Квалификация (степень) выпускника: | бакалавр |  |
| (бакалавр, магистр, специалист) |  |
|  |  | |
| Форма обучения: | очная |  |
| (очная, очно-заочная (вечерняя), заочная) |  |

г. Озёрск, 2021 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «*Защита данных*» являются:

• формирование знаний в области теоретических основ информационной безопасности;

• приобретение навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах;

• овладение техническими и программными средствами защиты информации при работе с персональным компьютером.

1. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Дисциплина «Защита данных» относится к математическому и естественно-научному циклу дисциплин основной образовательной программы бакалавриата по профилю «Информационно-измерительная техника и технологии». Для изучения дисциплины необходимо знание обязательного минимума содержания среднего (полного) образования по информатике.

1. КОМПЕТЕНЦИИ СТУДЕНТА, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ / ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ОБРАЗОВАНИЯ И КОМПЕТЕНЦИИ СТУДЕНТА ПО ЗАВЕРШЕНИИ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

В результате освоения данной дисциплины у студента формируются следующие компетенции:

|  |  |  |
| --- | --- | --- |
|  | **УК-1** | **Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач** |
|  | З-УК-1 | Знать: методики сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа |
|  | У-УК-1 | Уметь: применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников |
|  | В-УК-1 | Владеть: методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач |
|  | **УКЦ-2** | **Способен искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач** |
|  | З-УКЦ-2 | Знать: методики сбора и обработки информации с использованием цифровых средств, а также актуальные российские и зарубежные источники информации в сфере профессиональной деятельности, принципы, методы и средства решения стандартных задач профессиональной деятельности с использованием цифровых средств и с учетом основных требований информационной безопасности |
|  | У-УКЦ-2 | Уметь: применять методики поиска, сбора и обработки информации; с использованием цифровых средств, осуществлять критический анализ и синтез информации, полученной из разных источников, и решать стандартные задачи профессиональной деятельности с использованием цифровых средств и с учетом основных требований информационной безопасности |
|  | В-УКЦ-2 | Владеть: методами поиска, сбора и обработки, критического анализа и синтеза информации с использованием цифровых средств для решения поставленных задач, навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с использованием цифровых средств и с учетом требований информационной безопасности |
|  | **ОПК-4** | **Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности** |
|  | З-ОПК-4 | знать технические и программные средства реализации информационных технологий; знать современные программное обеспечение; знать основные методы и средства защиты информации. |
|  | У-ОПК-4 | уметь использовать возможности вычислительной техники, программного обеспечения, средств защиты информации для решения практических задач. |
|  | В-ОПК-4 | владеть навыками использования современных информационных технологий и программного обеспечения для решения задач профессиональной деятельности; владеть навыками соблюдения требований информационной безопасности при использовании современных информационных технологий и программного обеспечения. |

В результате освоения дисциплины студент должен:

• знать состояние и правовые основы информационной безопасности РФ, правовые гарантии информационной безопасности личности.

• уметь использовать действующее законодательство РФ в информационной сфере.

• владеть методами защиты информации.

• знать принципы криптографических преобразований, сертифицированные программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду;

• уметь реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации;

• иметь представление о сертифицированных разработанных средствах защиты информации и возможностях их использования в реальных задачах создания и внедрения информационных систем.

1. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет *3* кредита, *108* часов.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Общая трудоемкость дисциплины составляет: |  |  |  |  |
| Кредитов: | 3 |  |  |  |
| Часов (без учета часов на экзамен): | 108 |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Раздел учебной дисциплины | Недели | Виды учебной деятельности, включая СРС, трудоемкость (в часах) | | | | Текущий контроль успеваемости (*неделя, форма*) | Аттестация раздела  (*неделя, форма*) | Макс. балл за раздел |
| Лекции | Практ. занятия/ семинары | Лаб. раб. | СРС |
|  | 4 семестр | | | | | | | | |
| 1 | Основы информационной безопасности | 1-3 | 6 | 4 | 0 | 10 | 3КР1,  ПР1-3 | 17ДЗ3  3КР1 | 10 |
| 2 | Технические средства защиты данных | 4-7 | 8 | 4 | 0 | 10 | 6КР2  ПР4-7 | 6КР2  7ДЗ1 | 10 |
| 3 | Алгоритмы шифрования | 8-13 | 12 | 22 | 0 | 10 | 8-13ПР | 13ДЗ2 | 20 |
| 4 | Безопасность компьютерных сетей | 14-17 | 8 | 4 | 0 | 10 | ПР14-17 | 17ДЗ3 | 10 |
|  | Всего часов за семестр: |  | 34 | 34 | 0 | 40 |  |  |  |
|  | Итого баллов за 4 семестр: |  | 32 | 32 |  | 52 |  |  | 50 |
|  | Зачет: |  |  |  |  |  |  |  | 50 |
|  | Итого: |  |  |  |  |  |  |  | 100 |

Обозначения оценочных средств: ПР - практическая работа, КР - контрольная работа, ДЗ - индивидуальное домашнее задание.

Содержание разделов учебной дисциплины

|  |  |  |
| --- | --- | --- |
| № | Раздел учебной дисциплины | Содержание раздела |
| 1 | Основы информационной безопасности | Значение информации и ее защиты. Понятие информационной безопасности. Законодательные и правовые аспекты защиты информации. Обзор российского законодательства в области информационной безопасности. Организационные методы защиты данных. Классификация угроз информационной безопасности. Основные методы реализации угроз информационной безопасности. |
| 2 | Технические средства защиты данных | Методы и средства защиты информации в компьютерных системах. Идентификация и аутентификация. Общие подходы к построению парольных систем. Выбор паролей. |
| 3 | Алгоритмы шифрования | Шифрование данных. Типы алгоритмов шифрования. Симметричные алгоритмы шифрования. Ассиметричные алгоритмы шифрования. Криптографические средства обеспечения подлинности сообщений Электронно-цифровая подпись. Управление криптографическими ключами |
| 4 | Безопасность компьютерных сетей | Методы и средства защиты от удаленных атак через сеть internet. Защита информации в электронных платёжных системах. Обеспечение безопасности платежей через сеть internet. Программно-аппаратные средства защиты информации. |

1. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательный процесс по дисциплине строится на основе комбинации образовательных технологий. При освоении разделов дисциплины используется сочетание видов учебной деятельности (лекции, практические занятия, самостоятельная работа студента) с использованием интерактивных форм проведения занятий в аудитории.

Используемые образовательные технологии при изучении данной дисциплины:

- контекстное обучение;

- метод проектов;

- работа в команде;

- дискуссия;

- тренинг;

Интерактивные формы проведения занятий составляют 14 часов или 14% от общего объема аудиторных занятий.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ.

Текущий контроль проводится в виде контроля выполнения практических работ.

Примерные темы практических работ:

1. Информационные противостояния от древности до Нового времени. Информационные войны ХХ века
2. Защита сведений, составляющих государственную и коммерческую тайну, конфиденциальную информацию и интеллектуальную собственность
3. Обработка персональных данных. Информационная безопасность в повседневной жизни
4. Информационные и компьютерные преступления
5. Основные направления и мероприятия по защите электронной информации
6. Политика безопасности предприятия.
7. Защита данных в области атомной энергии
8. Оценка рисков информационной безопасности
9. Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей
10. Шифрование с использованием метода гаммирования
11. Классические алгоритмы подстановки и перестановки
12. Алгоритм симметричного шифрования aes rijndael
13. Современные алгоритмы шифрования и хэширования
14. Атака на алгоритм шифрования RSA
15. Электронная цифровая подпись
16. Изучение программных продуктов защиты данных.
17. Защита программного обеспечения методами стеганографии

6.2. Рубежный контроль (аттестация раздела) проводится в виде контрольных работ и индивидуальных домашних заданий.

6.2.1.

Контрольная работа № 1 «Основные понятия информационной безопасности».

Время проведения контрольной работы - 3 неделя.

* + 1. Контрольная работа № 2 «Методы и средства защиты информации»

Время проведения контрольной работы - 6 неделя.

* + 1. Индивидуальное домашнее задание № 1 «Реализация простейшего генератора паролей, обладающего требуемой стойкостью ко взлому»

Индивидуальное домашнее задание выдается на 4 неделе.

Срок сдачи индивидуального домашнего задания - 7 неделя.

* + 1. Индивидуальное домашнее задание № 2 «Криптоанализ классических шифров: шифр простой замены»

Индивидуальное домашнее задание выдается на 7 неделе.

Срок сдачи индивидуального домашнего задания - 13 неделя.

* + 1. Индивидуальное домашнее задание № 3 «Анализ рисков объекта защиты информации»

Индивидуальное домашнее задание выдается на 13 неделе.

Срок сдачи индивидуального домашнего задания - 17 неделя.

* 1. Аттестация выполняется в виде зачета.

Примерный перечень вопросов к зачету

1) Значение информации и ее защиты. Понятие информационной безопасности.

2) Роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ.

3) Правовое обеспечение информационной безопасности: виды информации по кате-гории доступа.

4) Правовое обеспечение информационной безопасности: правовой режим защиты государственной тайны. Степени и грифы секретности.

5) Виды конфиденциальной информации и режимы ее защиты.

6) Информационная война. Противоборствующие стороны в информационной войне. Признаки поражения в информационной войне.

7) Виды информационно-психологического оружия. Роль средств массовой информа-ции в ведении ИВ.

8) Классификация угроз информационной безопасности.

9) Основные методы реализации угроз информационной безопасности.

10) Методы нарушения конфиденциальности информации.

11) Методы нарушения целостности информации.

12) Методы нарушения доступности информации.

13) Вредоносное программное обеспечение

14) Организационные способы обеспечения ИБ: формы контроля и надзора за персо-налом

15) Организационные способы обеспечения ИБ: работа с кадрами и внутриобъектовый режим.

16) Организационные способы обеспечения ИБ: допуск к работе с конфиденциальной информацией.

17) Организационные способы обеспечения ИБ: режим учета и хранения веществен-ных носителей информации.

18) Технические способы обеспечения ИБ: шифрование и электронная цифровая под-пись.

19) Технические способы обеспечения ИБ: виды компьютерной стеганографии

20) Технические способы обеспечения ИБ: антивирусная защита информации.

21) Идентификация и аутентификация. Способы подтверждения подлинности и принад-лежности программ и данных.

22) Алгоритм симметричного шифрования ГОСТ 28147-89

23) Алгоритм симметричного шифрования DES

24) Алгоритм симметричного шифрования IDEA

25) Принцип работы ассиметричных алгоритмов шифрования

26) Алгоритм ассиметричного шифрования RSA

27) Алгоритм ассиметричного шифрования Диффи-Хеллмана

28) Алгоритм ассиметричного шифрования Эль Гамаля

29) Алгоритм ассиметричного шифрования ЕСС

30) Технология создания электронной подписи. Понятии хеш-функции

31) Алгоритм хэш-функции MD-4

32) Алгоритм хэш-функции SHA

33) Алгоритм хэш-функции ГОСТ 3411

34) Алгоритм цифровой подписи ГОСТ 3410

35) Алгоритм цифровой подписи DSA

36) Алгоритм цифровой подписи Эль Гамаля.

6.4. Самостоятельная работа студента

Самостоятельная работа студента заключается в подготовке к лекциям, практическим занятиям, контрольным работам и выполнении индивидуальных домашних заданий.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Семестр | Раздел учебной дисциплины | Виды СРС | Часов |
| 1 | 4 | Все | ПЛ1-ПЛ18, ПП1-ПП17 | 40 |
| 2 | 4 | Основы информационной безопасности | ДЗ3, ПК1 | 10 |
| 3 | 4 | Технические средства защиты данных | ДЗ1, ПК2 | 10 |
| 4 | 4 | Алгоритмы шифрования | ДЗ2 | 10 |
| 5 | 4 | Безопасность компьютерных сетей | ДЗ3 | 10 |

ДЗ — индивидуальное домашнее задание, ПЛ — подготовка к лекциям, ПП — подготовка к практическим занятиям, ПК — подготовка к контрольной работе.

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

* 1. Основная литература:

1. Баранова Е.К., Бабаш А.В. Криптографические методы защиты информации. Ла-бораторный практикум: учебное пособие + CD-ROM – М.: КНОРУС, 2015. —200с.
2. Белов Е.Б, Лось В.П. и др. Основы информационной безопасности. М.: Горячая линя - Телеком, 2006. — 544 с
3. Завгородний В.И. Комплексная защита информации в компьютерных системах.— М.: Логос, 2001. — 264 с.
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 2001.— 328 с.
5. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации.—М.: «Академия», 2008.—336с.
   1. дополнительная литература:

1) Скромбей Д., Шема М. Безопасность Web – приложений – готовые решения. — М.: Вильямс, 2003. — 386 с.

2) Соломаа А. Криптография с открытым ключом. — М.: Мир, 1995.— 318с.

3) Гульев И. Компьютерные вирусы.— М.: ДМК, 1998.— 304 с.

4) Шнайер Б. Прикладная криптография.— М.: Триумф, 2002. — 610 с.

8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Лекции проводятся в аудиторном классе, оборудованном доской, компьютером, мультимедийным проектором, экраном для проектора.

Практические занятия проводятся в компьютерном классе (11 компьютеров).

Требуемое программное обеспечение

|  |  |  |
| --- | --- | --- |
| № | Программный продукт | Количество |
| 1 | Операционная система Microsoft Windows XP, 7, 8, 10 | 1 шт. на компьютер |
| 2 | Программное обеспечение Microsoft Оffice 2010 | 1 шт. на компьютер |
| 3 | Файловый менеджер FAR | 1 шт. на компьютер |
| 4 | Программа для просмотра документов формата PDF | 1 шт. на компьютер |

Программа составлена в соответствии с требованиями ФГОС ВПО по направлению подготовки (специальности)*12.03.01 Приборостроение*

Автор(ы): *доцент кафедры Прикладной математики, к. пед. н.*

*Шеметова Анастасия Дмитриевна*

Рецензент(ы): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Программа одобрена на заседании\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_