|  |  |  |  |
| --- | --- | --- | --- |
| 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  «24» мая 2021 г. | | |
| РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ | | |
| Защита информации | | |
| (наименование дисциплины ) | | |
|  | | |
| Направление подготовки (специальность): |  | |
|  |  | |
| Профиль подготовки: |  | |
|  |  | |
| Наименование образовательной программы: |  | |
|  |  | |
| Квалификация (степень) выпускника: | бакалавр |  |
| (бакалавр, магистр, специалист) |  |
|  |  | |
| Форма обучения: |  |  |
| (очная, очно-заочная (вечерняя), заочная) |  |

г. Озёрск, 2021 г.

# ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины «Защита информации» является изучение:

- основных положений в области безопасности информации;

- сервисов обеспечения безопасности информации в автоматизированных системах;

- программно-аппаратных средств защиты информации;

- моделей разграничения доступа;

- организационных мер по защите информации;

- основных положений криптографии;

- алгоритмов шифрования;

- инфраструктуры открытых ключей;

- стадий и принципов построения автоматизированных систем в защищенном исполнении;

- распространенных угроз информационной безопасности;

- стандартов и положений в области защиты информации.

# МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Дисциплина «Защита информации» входит в Блок 1 «Дисциплины (модули)» в обязательную часть основной образовательной программы бакалавриата «Программное обеспечение средств вычислительной техники и автоматизированных систем», модуль «Общепрофессиональный».

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

В результате изучения дисциплины студент должен ЗНАТЬ:

- основные положения в области безопасности информации;

- сервисы обеспечения безопасности информации в автоматизированных системах;

- программно-аппаратные средств защиты информации;

- модели разграничения доступа;

- распространённые организационные мер по защите информации;

- основные положений криптографии;

- базовые алгоритмы шифрования;

- основные положения инфраструктуры открытых ключей;

- стадии и принципы построения автоматизированных систем в защищенном исполнении;

- распространенные угрозы информационной безопасности;

- стандарты и положений в области защиты информации.

В результате изучения дисциплины студент должен УМЕТЬ:

- определять и анализировать угрозы безопасности информации, а также составлять модель возможного нарушителя;

- использовать методы и средства защиты информации, а также аргументировать их выбор на основе модели угроз;

- разрабатывать и создавать типовые схемы защиты информации на основе современных средств защиты информации;

- пользоваться стандартами, нормативными правовыми актами из области безопасности информации при проектировании систем защиты.

В результате изучения дисциплины студент должен ВЛАДЕТЬ:

- методами выявления и анализа способов нарушения безопасности информации;

- навыками настройки штатных защитных средств современных операционных системы;

- навыками настройки средств защиты информации от несанкционированного доступа;

- подходами при построении автоматизированных систем в защищенном исполнении.

В результате освоения данной дисциплины у студента формируются следующие компетенции и планируются следующие результаты обучения по дисциплине:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Компетенция / Индикатор | Содержание | Результаты обучения по дисциплине |
|  | | **ОПК-3** | **Способен разрабатывать модели и компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии** |  |
|  | | ОПК-3.1 | З-ПК-3 Знать: схемотехнику логических схем, цифровых и запоминающих устройств, принципы построения и элементы микропроцессоров и микроконтроллеров, принципы работы программируемых логических матриц и программируемой матричной логики, основы объектно- ориентированного подхода к программированию, базы данных и системы управления базами данных для информационных систем различного назначения, принципы построения современных операционных систем и особенности их применения |  |
|  | | ОПК-3.2 | У-ПК-3 Уметь: строить логические схемы счетчиков, регистров, сумматоров и запоминающих устройств, строить временные диаграммы работы интерфейсов и контроллеров, сопрягать аппаратные и программные средства в составе аппаратно- программных комплексов, работать с современными системами программирования, включая объектно- ориентированные |  |
|  | | ОПК-3.3 | В-ПК-3 Владеть: современными инструментальными средствами проектирования цифровых устройств, языками процедурного и объектно- ориентированного программирования, навыками разработки и отладки программ |  |
|  | | **ОПК-4** | **Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью** |  |
|  | | ОПК-4.1 | З-ОПК-4 Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы |  |
|  | | ОПК-4.2 | У-ОПК-4 Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы |  |
|  | | ОПК-4.3 | В-ОПК-4 Владеть: составления технической документации на различных этапах жизненного цикла информационной системы |  |
|  | | **ПК-5.1** | **способен обеспечивать информационную безопасность в информационных системах, в том числе на уровне баз данных** |  |
|  | | ПК-5.1.1 | З-ПК-5.1 знать методы и средства защиты информации, в том числе на уровне баз данных, законодательство в сфере обеспечения безопасности информации |  |
|  | | ПК-5.1.2 | У-ПК-5.1 уметь применять методы и средства защиты информации в информационных системах и база данных в соответствии с установленными требованиями |  |
|  | | ПК-5.1.3 | В-ПК-5.1 владеть навыками защиты информации в информационных системах и базах данных, разработки документации в сфере информационной безопасности |  |
|  | | **ПК-5.3** | **способен разрабатывать требования и проектировать программное обеспечение** |  |
|  | | ПК-5.3.1 | З-ПК-5.3 знать принципы, технологии, подходы и инструменты, используемые при разработке математического, информационного, технического, лингвистического, программного, эргономического, организационного и правового обеспечения программного обеспечения средств вычислительной техники и автоматизированных систем |  |
|  | | ПК-5.3.2 | У-ПК-5.3 уметь разрабатывать требования к математическому, информационному, техническому, лингвистическому, программному, эргономическому, организационному и правовому обеспечению программного обеспечения средств вычислительной техники и автоматизированных систем, проектировать его |  |
|  | | ПК-5.3.3 | В-ПК-5.3 владеть навыками разработки требований к математическому, информационному, техническому, лингвистическому, программному, эргономическому, организационному и правовому обеспечению программного обеспечения средств вычислительной техники и автоматизированных систем, навыками следования этим требованиям |  |

# СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Общая трудоемкость дисциплины составляет | 3 | кредитов, |  |  |
| часов | 108 |  |  |  |

в том числе в 8 семестре: контактная работа 36 (лекции 18, практики 18), самостоятельная работа 36, контроль 36 (экзамен)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № 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 |
|  | 8 семестр |  |  |  |  |  |  |  |  |
| 1 | Основные положения защиты информации | 1-3 | 8 | 4 | 0 | 6 | 1-3ПР | 1ДЗ1 | 8 |
| 2 | Программно-аппаратные средства защиты информации | 4-7 | 6 | 10 | 0 | 8 | 4-7ПР | 7КР1 | 8 |
| 3 | Криптография | 8-11 | 6 | 10 | 0 | 8 | 8-11ПР | 16ДЗ2 | 9 |
| 4 | Организационные меры защиты информации. Средства физической защиты | 12-13 | 4 | 0 | 0 | 4 | 12-13ПР | 13КР2 | 9 |
| 5 | Стандарты и нормативно-правовые акт в области безопасности информации | 14-16 | 6 | 4 | 0 | 9 | 14-16ПР | 16КР3 | 8 |
| 6 | Построение автоматизированных систем в защищенном исполнении | 17-18 | 6 | 4 | 0 | 9 | 17-18ПР | 16КР3 | 8 |
|  | Всего часов: | 1-18 | 32 | 32 | 0 | 44 | 108 |  | 0 |
|  | Итого баллов за семестр: |  |  |  |  |  |  |  | 50 |
|  | Экзамен: |  |  |  |  |  |  |  | 50 |
|  | Итого за 8 семестр: |  |  |  |  |  |  |  | 100 |

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

Содержание разделов учебной дисциплины

|  |  |  |
| --- | --- | --- |
| № | Раздел учебной дисциплины | Содержание раздела |
| 1 | Основные положения защиты информации | Введение. Обзор лекций и практических занятий. Основные термины и понятия. Основные методы обеспечения информационной безопасности. Монитор безопасности. Идентификация, аутентификация. Дискреционная модель разграничения доступа. Мандатная модель разграничения доступа. Способы неявного представления матрицы доступа. Безопасность информационных потоков. Домен безопасности. |
| 2 | Программно-аппаратные средства защиты информации | Основные понятия. Средства идентификации и аутентификации. Доверенная загрузка системы. Замкнутая программная среда. Контроль целостности компонентов. Гарантированное удаление информации. Протоколирование и аудит. Межсетевой экран. Системы обнаружения атак и вторжений. |
| 3 | Криптография | Основные понятия. История развития криптографии. Классификация алгоритмов шифрования. Симметричные алгоритмы шифрования. Базовые операции в симметричных алгоритмах шифрования. Сеть Фейштеля. Ассиметричные алгоритмы шифрования. Инфраструктура открытых ключей. Электронно-цифровая подпись. |
| 4 | Организационные меры защиты информации. Физическая защиты | Основные понятия. Обзор основных организационных мер защиты информации. Общие правила обеспечения режима безопасности информации. Средства физической защиты. |
| 5 | Стандарты и нормативно-правовые акт в области безопасности информации | Классификация нормативной документации. История развития. «Оранжевая книга». Руководящие документы ФСТЭК России. Доктрина информационной безопасности РФ. Обзор нормативно-правовых актов РФ в области защиты информации. Руководящие документы Госкорпорации «Росатом» |
| 6 | Построение автоматизированных систем в защищенном исполнении | Классификация удаленных атак. Обзор распространённых атак. Компьютерные вирусы. Модель угроз. Модель нарушителя. Стадии построения автоматизированных систем в защищенном исполнении. Понятие аттестации объекта информатизации. Понятие сертификации средств защиты информации и специализированного ПО. |

# 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 20 часов или 28% 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. Управление пользователями и их правами к файлам и каталогам
2. Настройка парольной политики ОС семейства Microsoft Windows
3. Изучение и настройка политики безопасности ОС семейства Microsoft Windows
4. Изучение и настройка ограниченной программной среды средствами ОС семейства Microsoft Windows
5. Изучение процессов гарантированного удаления остаточной информации в файловой системе NTFS
6. Установка СЗИ от НСД Secret Net 6.5
7. Изучение базовых механизмов СЗИ от НСД Secret Net 6.5
8. Настройка замкнутой программной среды средствами СЗИ от НСД Secret Net 6.5
9. Настройка механизма контроля устройств и контроля целостности СЗИ от НСД Secret Net 6.5
10. Изучение мандатной модели разграничения доступа и контроля информационных потоков на примере СЗИ от НСД Secret Net 6.5
11. Изучение зашифрованной файловой системы EFS
12. Программирование основных операций и базовых алгоритмов шифрования

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

### Контрольная работа № 1.

Тема: Основные защитные механизмы.

Время проведения - 7 неделя.

Варианты контрольной работы:

1. идентификация и аутентификация
2. модели разграничения доступа
3. замкнутая программная среда и контроль целостности
4. межсетевой экран

### Контрольная работа № 2.

Тема: Криптография.

Время проведения - 13 неделя.

Варианты контрольной работы:

1. базовые операции симметричных алгоритмов шифрования
2. симметричные и ассиметричные алгоритмы шифрования

### Индивидуальное домашнее задание № 1.

Тема: Защита информации.

Задание выдается на 2 неделе. Срок сдачи задания - 6 неделя.

Варианты заданий:

1. Актуальность защиты информации в современных системах
2. Обзор статистики фактов утечки информации
3. История развития средств защиты информации

### Индивидуальное домашнее задание № 2.

Тема: Симметричные алгоритмы шифрования.

Задание выдается на 14 неделе. Срок сдачи задания - 16 неделя.

Варианты заданий:

1. Разработка программного обеспечения, реализующего симметричный алгоритм шифрования с применением сети Вейштеля
2. Реализация алгоритма DES

## Промежуточная аттестация выполняется в виде экзамена в 3 семестре.

Примерный перечень вопросов к экзамену

1. Понятие защиты информации в АС. Свойства защищаемой информации.
2. Физические средства защиты.
3. Основные методы обеспечения информационной безопасности.
4. Организационные меры защиты информации.
5. Идентификация и аутентификация.
6. Замкнутая программная среда.
7. Угрозы информационной безопасности. Классификация угроз. Понятие нарушителя.
8. Разграничение прав доступа. Понятие монитора безопасности.
9. Дискреционная модель разграничения доступа.
10. Протоколирование и аудит.
11. Стандарты в информационной безопасности: «Оранжевая книга».
12. Матрица доступа. Способы неявного представления матрицы доступа.
13. Мандатная модель разграничения доступа.
14. Стандарты в информационной безопасности: Руководящие документы ФСТЭК России.
15. Безопасность информационных потоков. Модель Белла - Ла Падуллы.
16. Межсетевое экранирование.
17. Построение автоматизированных систем в защищенном исполнении.
18. Системы обнаружения вторжений.
19. Построение систем защиты от угроз нарушения доступности информации.
20. Сеть Фейштеля.
21. Цифровая подпись.
22. Механизм доверенной загрузки операционной системы.
23. Инфраструктура цифровых сертификатов.
24. Основные операции алгоритмов симметричного шифрования.
25. Основные понятия криптографии. Классификация криптографических алгоритмов.
26. Классификация удаленных атак на распределенную вычислительную систему.
27. Алгоритмы симметричного и асимметричного шифрования.
28. Вредоносное программное обеспечение (вирусы). Классификация.
29. Основные виды сетевых атак.
30. . Методы гаммирования.
31. Программно-аппаратные средства защиты информации.
32. Методы перестановки в алгоритмах шифрования.

## Самостоятельная работа студента

|  |  |  |
| --- | --- | --- |
| Раздел учебной дисциплины | Виды СРС | Часов |
| 7 семестр |  |  |
| Все | ПЛ1-18, ПП1-18 | 27 |
| Защита информации | ДЗ1 | 5 |
| Основные защитные механизмы | ПК1 | 4 |
| Криптография | ПК2 | 4 |
| Симметричные алгоритмы шифрования | ДЗ-2 | 4 |
|  | Всего часов: | 44 |

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

## Основная литература:

Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Издательство «Феникс», 2008. - 254 с.

Петров В.А., Пискарев А.С., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. Учебное пособие М.: МИФИ, 1995. - 84 с.

Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. учреждений высш. проф. образования. М.: Издательский центр «Академия», 2013. - 336 с.

Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб: Наука и техника , 2004. -384 с.

## Дополнительная литература:

Панасенко С.П. Алгоритмы шифрования. Специальный справочник. СПб: БХВ-Петербург, 2009. -576 с.: ил.

# МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

## Лекции проводятся в аудиторном классе, оборудованном доской.

## 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 | Средство виртуализации | 1 шт. на компьютер |
| 3 | Среда программирования Microsoft Visual Studio .NET | 1 шт. на компьютер |
| 4 | Демо-версия СЗИ от НСД Secret Net 6.5 | 1 шт. на компьютер |
| 5 | Демо-версия СПО СГУ-2 | 1 шт. на компьютер |
| 6 | Универсальный HEX-редактор WinHEX | 1 шт. на компьютер |

Программа составлена в соответствии с требованиями ОС НИЯУ МИФИ по направлению подготовки (специальности):

|  |  |
| --- | --- |
| 09.03.01 Информатика и вычислительная техника | |
| Автор(ы) | А. В. Шарабрин |
| Рецензент(ы) | С.В. Князев, начальник отдела обработки информации СИТ ФГУП «ПО «Маяк» |
| Программа одобрена на заседании  методического совета кафедры | 24 мая 2021 г., протокол № 5 |