ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Петербургский государственный университет путей сообщения

Императора Александра I»

(ФГБОУ ВО ПГУПС)

Кафедра «Информатика и информационная безопасность»

**РАБОЧАЯ ПРОГРАММА**

*дисциплины*

«БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ» (Б1.Б.8)

для специальности

10.05.03 «Информационная безопасность автоматизированных систем»

по специализации

«Информационная безопасность автоматизированных системна транспорте»

Форма обучения – очная

Санкт-Петербург

2019



**1. Цели и задачи дисциплины**

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным от 01.12.2016, приказ № 1509по специальности 10.05.03 «Информационная безопасность автоматизированных систем» по специализации «Информационная безопасность автоматизированных систем на транспорте» по дисциплине «Безопасность операционных систем» (Б1.Б.8).

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других базовых дисциплин профессионального цикла в соответствии с требованиями, установленными федеральным государственным образовательным стандартом для формирования у выпускника профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности: научно-исследовательская, проектная, контрольно-аналитическая,организационно-управленческая, эксплуатационная и специализацией «Информационная безопасность автоматизированных систем на транспорте».

Для достижения поставленной цели определены следующие задачи изучения дисциплины:

* подготовка студента по разработанной в университете основной образовательной программе к успешной аттестации планируемых конечных результатов освоения дисциплины;
* подготовка студента к изучению дисциплин, определённых учебным планом в соответствии с указанными компетенциями;
* развитие социально-воспитательного компонента учебного процесса.

При изучении дисциплины решаются следующие конкретные задачи:

* изучение основных принципов построения, назначения и функций операционных систем;
* изучение управления задачами и ресурсами в операционных системах;
* изучение требований к защите операционных систем;
* изучение разграничения доступа в операционных системах;
* изучение аудита в операционных системах.

**2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы**

Планируемыми результатами обучения по дисциплине являются: приобретение знаний, умений, навыков и/или опыта деятельности.

В результате освоения дисциплины обучающийся должен:

**ЗНАТЬ:**

– принципы построения и функционирования, примеры реализаций современных операционных систем;

– функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами;

– критерии оценки эффективности и надежности средств защиты операционных систем;

– принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;

**УМЕТЬ:**

– использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;

– оценивать эффективность и надежность защиты операционных систем;

– планировать политику безопасности операционных систем;

**ВЛАДЕТЬ:**

– навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;

– навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности;

– навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.

Приобретенные знания, умения, навыки и/или опыт деятельности, характеризующие формирование компетенций, осваиваемые в данной дисциплине, позволяют решать профессиональные задачи, приведенные в соответствующем перечне по видам профессиональной деятельности в п. 2.4 основной профессиональной образовательной программы (ОПОП).

Изучение дисциплины направлено на формирование следующих **профессиональных компетенций (ПК)**, соответствующих видам профессиональной деятельности, на которые ориентирована программа специалитета:

*научно-исследовательская деятельность:*

– способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

– способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

*эксплуатационная деятельность:*

– способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-26).

Область профессиональной деятельности обучающихся, освоивших данную дисциплину, приведена в п. 2.1 ОПОП.

Объекты профессиональной деятельности обучающихся, освоивших данную дисциплину, приведены в п. 2.2 ОПОП.

**3. Место дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина «Безопасность операционных систем» (Б1.Б.8) относится к базовой части и является обязательной.

**4. Объем дисциплины и виды учебной работы**

|  |  |  |  |
| --- | --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестр** | |
| **5** | **6** |
| Контактная работа (по видам учебных занятий)  В том числе:   * лекции (Л) * практические занятия (ПЗ) * лабораторные работы (ЛР) | 148  66  16  66 | 64  32  32 | 84  34  16  34 |
| Самостоятельная работа (СРС) (всего) | 95 | 26 | 69 |
| Контроль | 45 | 36 | 9 |
| Форма контроля знаний | Э,З,КР | Э | З, КР |
| Общая трудоемкость: час / з.е. | 288/8 | 126/3,5 | 162/4,5 |

**5. Содержание и структура дисциплины**

5.1 Содержание дисциплины

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
|  | Модуль 1 | |
| 1 | Введение в операционные системы | Понятие операционной системы (ОС). Функции ОС. Эволюция ОС. Виды ОС.  Многозадачность. Понятие многозадачности. Виды многозадачности. |
| 2 | Процессы и потоки | Многозадачность, мультипроцессирование и мультипрограммирование.  Понятие процесса. Состояние процессов.  Создание процессов и потоков. Описатель процесса. Потоки-потомки.  Алгоритмы планирования на основе приоритетов и квантования на примере ОС Unix, Linux, Windows.  Прерывания: определение, виды, основные особенности. Механизмы обработки прерываний. Системные вызовы.  Проблема неопределенности параллелизма. Синхронизация процессов и потоков. Использование блокирующих переменных. Синхронизация процессов и потоков. Блокировка системным вызовом. Синхронизация процессов и потоков. Семафоры. Синхронизация процессов и потоков. Тупиковые ситуации. |
| 3 | Управление памятью | Функции ОС по управлению памятью.  Алгоритмы распределения памяти. Распределение памяти фиксированными разделами. Распределение памяти динамическими разделами. Распределение памяти перемещаемыми разделами.  Типы адресов памяти. Свопинг и виртуальная память.  Страничное распределение памяти. Организация адресного пространства при страничном распределении. Особенности преобразования виртуальных адресов. Стратегии выбора страниц для выгрузки и загрузки. Способы оптимизации.  Сегментное распределение памяти.  Сегментно-страничное распределение памяти: организация адресного пространства, преобразование виртуального адреса.  Разделяемые сегменты памяти. |
| 4 | Файловая система | Понятие файла. Структурированные и неструктурированные файлы.  Файловая система и ее функции.  Физическая организация файловой системы.  Способы физического размещения файла. Особенности файловой системы FAT.  Способы физического размещения файла. Особенности файловой системы NTFS. |
| 5 | Концепции распределенной обработки в сетевых ОС | Понятие сетевых и распределенных ОС. Цели применения.  Функциональные компоненты сетевой ОС.  Сетевые службы и сетевые сервисы.  Одноранговые и серверные сетевые ОС.  Концепция распределенного приложения.  Передача сообщений в распределенных системах. Способы адресации при передаче сообщений.  Передача сообщений в распределенных системах. Механизм сокетов. |
|  | Модуль 2 | |
| 6 | Угрозы безопасности ОС | Классификация угроз безопасности ОС.  Типовые атаки на операционные системы: сборка «мусора», сканирование файловой системы, превышение полномочий пользователей.  Типовые атаки на операционные системы: атаки на пароли, использование программных закладок, «жадные» программы.  Понятие безопасной операционной системы. Подходы к построению защищенных операционных систем. |
| 7 | Типовая архитектура подсистемы защиты ОС | Идентификация и аутентификация пользователей операционной системы.  Разграничение доступа к объектам ОС. Избирательное (дискреционное) разграничение доступа. Изолированная программная среда. Полномочное разграничение доступа без контроля и с контролем информационных потоков.  Аудит безопасности ОС. |
| 8 | Особенности защиты в операционных системах семейства UNIX | Иерархия пользователей и групп системы UNIX.  Хранение информации о пользователях и группах в Unix-подобных системах.  Подсистема идентификации и аутентификации в ОС Unix.  Особенности работы с файлом теневых паролей в ОС Unix. Подключаемые модули аутентификации.  Подсистема разграничения доступа в ОС Unix. Концепция разграничения доступа к ресурсам. Атрибуты безопасности.  Подсистема аудита в ОС Unix.  Защита целостности структур ядра в ОС Unix. |
| 9 | Особенности защиты в операционных системах семейства WINDOWS | Подсистема идентификации и аутентификации в ОС Windows. Архитектура подсистемы аутентификации. Параметры аутентификации.  Подсистема разграничения доступа в ОС Windows. Объекты доступа. Субъекты доступа. Методы доступа и права доступа к объектам. Привилегии.  Атрибуты безопасности пользователя. Идентификатор безопасности пользователя. Маркер доступа пользователя. Дескриптор защиты.  Подсистема аудита. |

5.2 Разделы дисциплины и виды занятий

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** |
| 1 | Введение в операционные системы | 4 |  |  | 2 |
| 2 | Процессы и потоки | 10 |  | 10 | 8 |
| 3 | Управление памятью | 8 |  | 10 | 8 |
| 4 | Файловая система | 4 |  | 6 | 4 |
| 5 | Концепции распределенной обработки в сетевых ОС | 6 |  | 6 | 4 |
| 6 | Угрозы безопасности ОС | 4 | 4 |  | 10 |
| 7 | Типовая архитектура подсистемы защиты ОС | 8 | 12 |  | 11 |
| 8 | Особенности защиты в операционных системах семейства UNIX | 10 |  | 34 | 24 |
| 9 | Особенности защиты в операционных системах семейства WINDOWS | 12 |  |  | 24 |
| **Итого** | | 66 | 16 | 66 | 95 |

**6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

Перечень методического обеспечения по всем разделам дисциплины представлен в документе «Источники теоретического материала для лекций» и методических рекомендациях по организации самостоятельной работы обучающихся, включенных в состав методических материалов дисциплины.

**7. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине**

Фонд оценочных средств по дисциплине является неотъемлемой частью рабочей программы и представлен отдельным документом, рассмотренным на заседании кафедры и утвержденным заведующим кафедрой.

**8. Перечень основной и дополнительной учебной литературы, нормативно-правовой документации и других изданий, необходимых для освоения дисциплины**

8.1 Перечень основной учебной литературы, необходимой для освоения дисциплины

1. Коньков, К. А. Основы операционных систем [Электронный ресурс] / К. А. Коньков, В. Е. Карпов. — 2-е изд. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 346 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/73693.html

2. Диасамидзе С. В. Безопасность операционных систем: учебное пособие. – СПб: ПГУПС, 2018. – 75 с.

3. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. [Электронный ресурс] — Электрон.дан. — М. : ДМК Пресс, 2012. — 592 с. — Режим доступа: <http://e.lanbook.com/book/3032>

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Войтов, Н.М. Основы работы с Linux. Учебный курс. [Электронный ресурс] — Электрон.дан. — М. : ДМК Пресс, 2010. — 216 с. — Режим доступа: <http://e.lanbook.com/book/1198>

2. Нортон, П. Полное руководство по Microsoft Windows XP. [Электронный ресурс] / П. Нортон, Д. Мюллер. — Электрон.дан. — М. : ДМК Пресс, 2009. — 733 с. — Режим доступа: <http://e.lanbook.com/book/1195>

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

При освоении данной дисциплины нормативно-правовая документация не используется.

8.4 Другие издания, необходимые для освоения дисциплины

При освоении данной дисциплины другие издания не используются.

**9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

1. Сайт научно-технической библиотеки университета: <http://library.pgups.ru/jirbis/index.php?option=com_irbis&Itemid=300>
2. Проект «Информационная безопасность». <http://www.itsec.ru/>
3. Проект IT <http://citforum.ru/>
4. Проект «Национальный Открытый Университет «ИНТУИТ»http://www.intuit.ru/

**10. Методические указания для обучающихся по освоению дисциплины**

Порядок изучения дисциплины следующий:

1. Освоение разделов дисциплины производится в порядке, приведенном в разделе 5 «Содержание и структура дисциплины». Обучающийся должен освоить все разделы дисциплины с помощью учебно-методического обеспечения, приведенного в разделах 6, 8 и 9 рабочей программы.
2. Для формирования компетенций обучающийся должен представить выполненные типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, предусмотренные текущим контролем (см. фонд оценочных средств по дисциплине).
3. По итогам текущего контроля по дисциплине, обучающийся должен пройти промежуточную аттестацию (см. фонд оценочных средств по дисциплине).

**11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем**

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине:

* персональные компьютеры, локальная вычислительная сеть кафедры, проектор;
* методы обучения с использованием информационных технологий: компьютерный лабораторный практикум, демонстрация мультимедийныхматериалов;
* лабораторное программное обеспечение, разрабатываемое в ходе учебного процесса студентами совместно с преподавателем;
* Интернет-сервисы и электронные ресурсы: сайты, перечисленные в разделе 9 рабочей программы; электронные учебно-методические материалы, доступные через личный кабинет обучающегося на сайте sdo.pgups.ru; на выбор обучающегося – поисковыесистемы, профессиональные, тематические чаты ифорумы, системы аудио и видео конференций, онлайн-энциклопедии исправочники.

Кафедра обеспечена необходимым комплектом лицензионного программного обеспечения:

* операционная система Windows Server, операционная система Windows, MS Office, Антивирус Касперский;
* Microsoft Visual C++ Express Edition (бесплатное, свободно распространяемое программное обеспечение, режим доступа https://www.microsoft.com/en-us/download/details.aspx?id=13276);
* VirtualBox (бесплатное, свободно распространяемое программное обеспечение, режим доступа <https://www.virtualbox.org>).

**12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Материально-техническая база обеспечивает проведение всех видов учебных занятий, предусмотренных учебным планом по данной специальности, и соответствует действующим санитарным и противопожарным нормам и правилам.

Она содержит специальные помещения, укомплектованных специализированной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Материально-техническая база дисциплины включает:

* помещения для проведения лекционных занятий, укомплектованные наборами демонстрационного оборудования (стационарными или переносными персональными компьютерами, настенными или переносными экранами, мультимедийными проекторами с дистанционным управлением и другими информационно-демонстрационными средствами) и учебно-наглядными пособиями (презентациями), обеспечивающими тематические иллюстрации в соответствии с рабочей программой дисциплины;
* лабораторию программно-аппаратных средств обеспечения информационной безопасности (ауд. 2-105), оснащенную программно-аппаратными средствами защиты информации в соответствии с требованиями ФГОС ВО; лаборатория также оборудована современной вычислительной техникой, комплектом проекционного оборудования для преподавателя;
* помещения для выполнения курсовой работы, оснащенные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых для выполнения индивидуального задания программных средств (см. раздел 11), а также комплектом оборудования для печати;
* помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации;
* помещения для проведения групповых и индивидуальных консультаций, укомплектованные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых программных средств (см. раздел 11);

